Mikko Pauna & Sami Ruotsalainen

TIETOTURVATYÖ PK-YRITYKSESSÄ

TIETOTURVATYÖ PK-YRITYKSESSÄ

Mikko Pauna
Sami Ruotsalainen
TIK8SNB
Opinnäytetyö
Syksy 2012
Tietojenkäsittelyn koulutusohjelma
Oulun seudun ammattikorkeakoulu

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

Tekijä(t): Mikko Pauna, Sami Ruotsalainen
Opinnäytetyön nimi: Tietoturvatyö PK-yrityksessä
Työn ohjaaja(t): Päivi Oja
Työn valmistumislukukausi ja -vuosi: Syksy 2012 Sivumäärä: 61

Tässä opinnäytetyössä perehdyttiin aluksi yleisesti tietoturvakartoitukseen, sekä sen hyötyihin että haasteisiin. Tutkimme, miten tietoturvakartoitus yleensä tehdään yritykselle. Tästä siirryttiin kartoittamaan kohdeyrityksen tietoturvan tilaa, niin sen hallinnollista kuin teknologistakin puolta, jotta pystyttiin määrittelemään miten sitä voitaisiin parantamaan juuri kohdeyritykselle sopivalla tavalla. Kartoituksen jälkeen alettiin etsimään sopivia keinoja, joilla havaittuja heikkoja kohtia voitaisiin päivittää ja parantaa. Uudistuksissa tulee perehtyä huolellisesti erilaisiin tietoturvaratkaisuihin, jotta muutokset toteutuvat kustannustehokkaasti ja toimintavarmasti.

Jo työn alussa meille tehtiin selväksi tyytymättömyys nykyisen sopimuksen tilaan ja tämä johti palveluntarjoajan vaihtamiseen. Toisen valtakunnallisen palveluntarjoajan lisäksi etsimme tarjouksen myös yksityiseltä yritykseltä, jotta tarjouksia voitaisiin vertailla ja siten valita kohdeyritykselle niistä sopivin. Yksityiseltä tullut tarjous oli samankaltainen aiemman sopimuksen kanssa, joten valtakunnalliselta saatu tarjous oli enemmän toimeksiantajamme mieleen.

Tietoturvakartoitus poikkeaa normaalin kartoituksen käytännöistä sillä tavoin, ettemme opinnäytetyön resurssien puitteissa kyenneet totetuttamaan esille tulleita parannuksia, vaan annoimme vain ehdotuksen siitä mitä kohennettavaa kohdeyrityksen tietoturvassa on.

Asiasanat: Tietoturva, Tietoturvakartoitus, Palomuuri, Virustorjunta,

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information Technology

Author(s): Mikko Pauna, Sami Ruotsalainen
Title of thesis: Tietoturvatyö PK-yrityksessä
Supervisor(s): Päivi Oja
Term and year when the thesis was submitted: Autumn 2012 Number of pages: 61

The goal of the thesis was to provide an information security survey to a midsized company which wasn't sure how their business was being handled in the matter. First thing done was to get familiar with the basics of the security survey by studying it vastly. Next we carried out a small investigation to the company's local office to see the main things to improve are, whether it's the management style or some sort of technological issue that could bring the whole company at risk. In this manner we discovered our objectives and how to start the work.

The report of the thesis starts with a short introduction to the main issue and continues with general knowledge about information security, the security survey and their content. After the introduction responsibilities and objectives that make up information security are sift through. This covers things such as information security plan, risk plan, and instructions for data security. The rest discusses the main subject; information security upgrading plan, it's usefulness for the target company, how things are currently handled and what could be done better. Last two chapters consist of deliberations and summary.

Keywords: Data Security, Firewall,

SANASTO JA LYHENTEET

VPN	(Virtual Private Network) Näennäisesti yksityinen verkko.
IPsec	(Internet Protocol Security) Tietoliikenteen salausprotokolla.
802.1Q	Lähiverkon standardi, jolla tarkoitetaan virtuaalilähiverkkoja tukevia laitteita.
UPS	(Uninterruptible Power Supply) Laite, jonka tarkoitus on turvata virransaanti lyhyiden sähkökatkojen ajan.
IDS	(Intrusion Detection System) Laite tai ohjelma, jonka tarkoitus on seurata verkon toimintaa ja estää siihen kohdistuvia tunkeutumisyrityksiä.
WLAN	(Wireless Local Area Network) Lähiverkkotekniikka, jonka avulla pystytään yhdistämään verkkolaitteet langattomasti Internetiin.
WEP/WPA/WPA2	Tiedonsalausmenetelmiä langattomassa lähiverkossa.
SSL	(Secure Sockets Layer) Salausmenetelmä käyttäjän Internet-selaimen ja palvelimen välillä.
HTTP	(Hypertext Transfer Protocol) Tiedonsiirtoprotokolla.

SISÄLLYS

1 JOHDANTO

Opinnäytetyön toimeksiantaja on oululainen perheryritys, joka haluaa pysyä nimettömänä. Työ keskittyy pääosin yrityksen Oulun alueella sijaitsevaan toimipisteeseen ja sen tietoturvaan. Opinnäytetyön tarkoituksena on kartoittaa kohdeyrityksen tietoturvan nykyinen taso ja saatujen tuloksien perusteella tehdä yritykselle ehdotus sen parantamiseksi, jotta yrityksen tietoturva saataisiin vastaamaan paremmin haluttuja vaatimuksia. Tietoturvakartoitus räätälöidään juuri kyseisen toimipisteen tarpeisiin sopivaksi, rajaten muut toimipisteet kokonaan pois. Näin opinnäytetyön laajuus pysyy hallittuna.

Opinnäytetyö alkaa yleisellä teorialla yritysten tietoturvasta, jonka jälkeen siirrytään tietoturvan tarkempaan kuvaukseen, aina työtehtävistä tietoverkkojen infrastruktuuriin. Sen jälkeen kartoitetaan yrityksen nykyistä tilaa empiirisellä evaluatiivisella (arvioivalla) tutkimuksella, johon sisältyy muun muassa toimitilojen laitteiston ja käyttöjärjestelmien määrittelyä. Kartoituksen perusteella pyritään päättelemään miten erilaiset tietoturvaratkaisut vaikuttaisivat yrityksen toimintaan ja mikä olisi paras valinta uudeksi suojaukseksi. Saatujen tarjouksien ja ratkaisujen vertailuiden tuloksista lisää kappaleessa 4.

Toimeksianto sisältää yrityksen tietoturvaan liittyviä arkaluonteisia tietoja. Näiden tietojen luottamuksellisina säilymisen varmistaaksemme olemme allekirjoittaneet salassapitosopimuksen, joka pätee myös opinnäytetyön valmistuttua. Yrityksen yhteyshenkilö toivoi myös työssä kiinnitettävän erityistä huomiota vanhentuneen palomuuritekniikan uusimiseen. Teimmekin toiveen pohjalta kokonaisen yksin palomuuriin keskittyvän luvun. Lisäksi sovimme myös tekevämme henkilökunnan toimistoon yleisen ohjeen. Henkilökunnalle suunnatussa ohjeessa käsitellään jokaisen työntekijän henkilökohtaista tietovastuuta, jottei työntekijöille ole epäselvää, miten esimerkiksi verkossa toimitaan vaarantamatta yrityksen toimintaa. Ennestään toimistolla ei tällaista ohjetta ollut ja ohje pyrittiin tekemään yritykselle kohdennetusti sen toiminta huomioon ottaen.

Raportissa käsitellään tietoturvaa ja sen eri osa-alueita, jonka jälkeen siirrytään itse kartoitukseen ja sen tuloksiin. Tämän jälkeen tulevat lopulliset johtopäätökset ja ehdotukset turvan parantamiseksi. Kirjalliset lähteet ja Internet-linkit ovat suurin osa työn tietoperustaa ja raportin teoria rakentuu suurimmaksi osaksi niistä. Työn toiminnallisessa osiossa hyödynnetään eri tiedonkeruumenetelmiä keräten mahdollisimman paljon tietoa kohdeyrityksen tietoturvan nykytilasta. Tiedonkeruumenetelmiä ovat esimerkiksi haastattelut, osallistuva havainnointi ja tilannetiedonhankinta, joista jälkimmäisten avulla kerättiin tietoa lähinnä yrityksen toimipisteen tilasta. Kartoitettuamme yrityksen tietoturvan nykytilan ja mahdolliset haavoittuvuudet luomme suunnitelman, jonka pohjalta tietoturva voidaan nostaa vaadittavalle tasolle. Työn tavoite on kartoittaa kohdeorganisaation tietoturvan nykyaso ja kartoituksessa ilmenneiden tietojen pohjalta ehdottaa yritykselle parempia tapoja hoitaa tietoturvallisuutta.

2 TIETOTURVA

2.1 Tietoturvan merkitys

Tietoturvan tavoitteena on suojata tietojärjestelmä niin, että sitä pystytään suojamaan niin tunnetuilta kuin tuntemattomiltakin uhilta. Tietojärjestelmän tietojen on myös oltava käytettävissä aina kun niiden käyttämiseen oikeutettu käyttäjä sitä haluaa. Tietoturvasta puhuttaessa se mielletään yleensä palomuurin ja virustorjuntaohjelman asentamiseksi työasemaan. Nämä toki liittyvät tietoturvaan, mutta ovat vain pieniä osia isosta kokonaisuudesta. Tietoturva käsittää kaiken mikä liittyy mm. tietojen saatavuuteen, oikeellisuuteen ja luotettavuuteen, kiistämättömyyteen ja todennukseen. (Ruohonen, 2002, 2.)

Tietovarat ovat tärkeä resurssi nykyajan liikemaailmassa ja ne tulee suojata asianmukaisella tavalla, ottaen huomioon tietoturvallisuuden perusasiat, jotka voidaan jakaa kolmeen osaan. Tietoaineiston on oltava:
1. saatavilla, eli sen on oltava käytettävissä silloin kuin sitä tarvitaan.
2. luottamuksellista, eli sitä voi käsitellä vain asianosaiset, tunnukset omaavat ihmiset.
3. eheää, eli tieto ei saa muuttua tarkoituksetta tai erilaisten hyökkäysten takia. (Laaksonen, Nevasalo, Tomula 2007, 17-18.)

Tiedon eheyden tavoitteena on, että tieto säilyy alkuperäisessä tarkoituksessaan, eikä tieto pääse muuttumaan matkan varrella tahattomasti tai tahallisesti. Hallitsemattomalla muutoksella tarkoitetaan jo olemassa olevan tiedon tuhoutumista tai uuden tiedon lisäämistä. Laajemmaassa tulkinnassa eheyden voidaan katsoa sisältävän myös sen, että tieto on oikeata eikä sisällä virheitä. (Hakala, 2006, 4.) Tiedon eheys voidaan menettää esimerkiksi kiintolevyn rikkoutumisessa tai krakkerin päästessä järjestelmän sisään tuhoamaan tietoja (Järvinen, 2002, 22-23).

Tiedon eheyden säilyttämiseksi on olemassa eri keinoja, joista yksi on lisätä tietoon yksisuuntaisella menetelmällä luotu tarkistussumma. Tiedon eheys

voidaan varmistaa tarkistussumman uudelleen laskemisella ja vertaamalla saatua tulosta viestin tarkisteeseen. Tarkisteen eheys täytyy varmistaa käyttämällä luottamuksellista avainta tarkistussumman luomiseen. Tarkistussummaa käytetään esimerkiksi tietoverkossa siirrettävän, järjestelmään tallennetun tai pakatun tiedon eheyden takaamiseksi. (Stallings 2006, 324-328.)

Tiedon saatavuudella tarkoitetaan, että tietoa pystyvät hyödyntämään siihen oikeutetut henkilöt aina niin halutessaan. Tieto täytyy varastoida sellaiseen paikkaan ja sellaiseen muotoon, että se on nopeasti hyödynnettävissä. Tiedon saatavuus voi vaarantua esimerkiksi, kun yrityksen tietojärjestelmää vastaan kohdistetaan palvelunestohyökkäys ja yrityksen tietoliikenne saadaan täysin jumiin ohjaamalla sinne ylimääräistä liikennettä. Huomattavasti yleisempi tapahtuma on esimerkiksi aktiivilaitteen rikkoutuminen, joka aiheuttaa vähintään hetkellisen katkon tiedon saatavuuteen. Tiedon saatavuuden turvatakseen yrityksen kannattaa huolehtia varmuuskopioinneista, sekä harkita esimerkiksi UPS-laitteiden käyttöönottoa kriittisissä paikoissa, ja lisäksi varautua tietoliikenteen toimimattomuuteen jo verkkoa suunniteltaessa. (Hakala M & Vainio M & Vuorinen O. 2006, 4.)

Luottamuksellisuudella tarkoitetaan sitä, että tietoon pääsevät käsiksi vain siihen oikeutetut henkilöt. Jos tietojärjestelmän käyttäjä pääsee käsiksi sellaiseen tietoon, johon hän ei ole oikeutettu tai ulkopuolinen hakkeri onnistuu murtautumaan yrityksen tietojärjestelmään, on luottamuksellisuus menetetty. Luottamuksellisuutta voidaan parantaa suojaamalla tieto esimerkiksi salasanalla, salakirjoittaa eli kryptata tieto tai sijoittaa ohjelmaan valvottuja takaportteja tunkeutujien ilmisaamiseksi. (Hakala M & al. 2006, 4.)

Kiistämättömyyden tavoite on pystyä todistamaan kaikki tietojärjestelmässä tapahtuneet teot. Sähköisessä kaupankäynnissä kiistämättömyys on tärkeä osa kaupantekoa. Myyjän täytyy pystyä todistamaan, että asiakas on tehnyt tilauksen ja että tuote on myös toimitettu asiakkaalle. (Hakala M & al, 2006, 5.)

Todennuksen avulla varmistetaan, että olio on se mikä hän esittääkin. Arkielämässä todennusta tapahtuu kokoajan, tunnistamme vastaantulevan henkilön hänen ulkonäkönsä perusteella. Oliolla voidaan tarkoittaa esimerkiksi henkilöä, laitetta, tietoa tai tapahtumaa. Yksilö voidaan todentaa esimerkiksi yksilöllisten ominaisuuksien, eli biometrisen tunnistuksen avulla. Todennus voidaan tehdä myös sillä perusteella mitä joku tietää, tarkoittaen esimerkiksi salasanaa tai PIN-koodia. Tunnistus voidaan tehdä myös sen perusteella mitä jollakulla on hallussaan, esimerkiksi älykortin perusteella. Pääsynvalvonnan tarkoitus on päästää järjestelmään vain ne todennetut henkilöt, jotka ovat siihen oikeutettuja. Pääsynvalvonnan piiriin kuuluu myös se miten järjestelmää käytetään sekä lokitiedostojen luominen. Lokitiedostot pitävät sisällään tietoa käyttäjistä jotka ovat avanneet, muokanneet tai tuhonneet tiedostoja. Suurin hyöty lokitiedoista on silloin kun tutkitaan tietoturvarikkomusta ja pitää saada selkeä käsitys siitä mitä on tapahtunut. (Järvinen, 2002, 27.)

Yritysten toiminta perustuu nykyaikana laajasti erilaisiin sähköisiin prosesseihin ja tärkeimmät tiedot ovat niiden koosta riippumatta säilöttyinä sähköisiin dokumentteihin. Nämä jokapäiväiseen toimintaan ja omaan osaamiseen liittyvät, yrityksen tärkeimmät tiedot ovat keskitetty erilaisiin tietojärjestelmiin, joissa niihin on helppo päästä käsiksi ja niitä on helppo hyödyntää. Nämä tietovarat ovat elintärkeitä yrityksen toimivuuden, kilpailun ja liikevaihdon kannalta. Lisäksi tieto tulee asettaa erilaisiin tärkeysluokkiin sen mukaan, mitä eri kriteerejä tieto milloinkin täyttää; esimerkiksi kuinka kriittistä tieto on liiketoiminnan kannalta. Näin suojataan tieto järkevästi ja kustannustehokkaasti, eikä tietoturvatyö ole ylimitoitettua. Tietoturvatyöstä ei näin tule sen turvaamaan sisältöön ja toimintaan nähden liian monimutkainen. (Ruohonen, 2002, 2.)

Yrityksen näkökulmasta ajatellen tietoturvan tarkoitus on turvata yrityksen liiketoiminta ja varmistaa sisäisten ja ulkoisten vaatimusten täyttyminen. Hyvä yritys ymmärtää tietoturvallisuuden kuuluvan kiinteänä osana nykyiseen organisaatiokulttuuriin. Siinä työntekijät pyrkivät ylläpitämään hyvää tietoturvallisuuden tasoa. Tietoturvallisuuden tekniset ja hallinnolliset toimenpiteet täytyy järjestää niin, että ne toteuttavat sille asetetut lainsäädännön määräykset ja rajoitukset, ja myöhemmin tulee seurata millä tavoin

tietoturvallisuuden ylläpitämisessä on onnistuttu. Sekä kotimainen että kansainvälinen lainsäädäntö luovat yrityksille suoria ja epäsuoria velvoitteita huolehtia tietoturvastaan. Nämä määritellyt velvoitteet ovat kuitenkin usein yleisluonteisia ja niiden käytännön toteutus jää yrityksen omalle vastuulle. Myös riittävä tietoturvan tason määrittäminen on yrityksen itsensä päätettävissä. Lainsäädännön lisäksi tulee muistaa esimerkiksi yritysten keskinäisiin sopimuksiin liittyvät tietoturvavelvoitteet. (Laaksonen & al, 2007, 17-18.)

Optimaalisen tietoturvan tason saavuttaminen vaatii yritykseltä määrätietoista toimintaa ja hyvää johtamista. Yrityksen ei tulisi nähdä tietoturvaan panostamista hukkaan heitettynä resurssina, jonka ainoa tarkoitus on aiheuttaa työntekijöille ylimääräistä vaivaa. Hyvin hoidettuna se on ennemminkin kilpailuvaltti. Tällaisilla oikeilla linjauksilla yrityksen liiketoiminnan jatkuvuus on hyvin turvattu, kun koko liiketoimintaympäristö noudattaa samaa tietoturvakulttuuria. Tietoturvallisuuden suhteen tehdyt ratkaisut voivat vaikuttaa liiketoimintaan hyvin suoraviivaisesti, jos esimerkiksi liikekumppanilla on kovia vaatimuksia tietoturvan suhteen, eikä se koe tulevan kumppaninsa tekemää tietoturvatyötä tarpeeksi kattavaksi luotettavan liikekumppanuustoiminnan kannalta.

Yritykset yrittävät usein parantaa tietoturvaansa liiaksi erilaisilla teknispainotteisilla toimenpiteillä sen sijaan, että yritys kouluttaisi henkilöstöä ja yrittäisi tätä kautta kehittää tietoturvallisuuden tasoaan. Päivittäisessä työssään työntekijät luovat ja käsittelevät tietoa ja ovat näin olennaisessa asemassa tietoturvan toteutumisessa. Osa heidän käsittelemästään tiedosta on peräisin asiakkaiden ja alihankkijoiden tiedoista ja näitä tietoja yhdistellään ja prosessoidaan erilaisilla tietojenkäsittelyvälineillä. Näiden käsiteltävien tietojen tunnistaminen on edellytys sille, että ne voidaan suojata tuhoutumiselta tai epäasialliselta käsittelyltä. (Laaksonen & al, 2007, 18-19.)

2.2 Tietoturvan osa-alueet

Tietoturvan osa-alueet:

- Hallinnollinen turvallisuus
- Tietoaineiston turvallisuus
- Henkilöstöturvallisuus
- Käyttöturvallisuus
- Tietoliikenneturvallisuus
- Fyysinen tietoturvallisuus
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus

Hallinnollinen turvallisuus liittyy tietojärjestelmän johtamiseen. Tavoitteena on varmistaa, että tietoturvan kaikki osa-alueet ovat riittävän hyvin suojattu. Myös tietoturvasuunnitelma kuuluu hallinnolliseen turvallisuuteen ja tavoitteena on varmistaa tietoturvan jatkuva ylläpitäminen ja kehittäminen. (Ruohonen, 2002, 5.)

Tietoturvallisuus ja sen johtaminen voidaan ymmärtää monella eri tavalla. Suppeimmillaan kyse voi olla tietoturvan huomioimisesta vain siinä määrin, että se täyttää lain tai tarpeiden minimivaatimukset. Asia laajemmin nähtäessä nimetään esimerkiksi tietoturvapäällikkö, jonka vastuualueena on koko tietoturvan hallinnointi. Isomman mittakaavan tietoturvajohtamisessa kyseessä voi olla täysin uusi tehtäväkokonaisuus, johon kuuluu sekä liiketoiminnan että tietohallinnon johtamista. Tietoturvallisuuden johtamiseen on kehitetty erilaisia viitekehyksiä, standardeja ja malleja jotka tunnetaan ”alan parhaina käytäntöinä”. Sen lisäksi on olemassa erilaisia muistilistoja ja dokumentteja, jotka auttavat hahmottamaan tietoturvallisuuden osa-alueita. Niiden tarkoitus on tuoda selkeyttä tietoturvaan liittyviin käytäntöihin. Paras hyöty niistä saadaan silloin, kun tietoturvallisuus on läsnä koko organisaation päivittäisessä toiminnassa, niin työntekijöiden kuin johtamisenkin suhteen. (Laaksonen & al, 2006, 115.)

Tietoaineiston turvallisuus käsittää tietojärjestelmän tiedostot. Usein ajatellaan tietoturvan koostuvan vain näistä. Tietoaineiston turvallisuus riippuu mm. virustorjuntaohjelmista, varmuuskopioinnista sekä käyttöoikeuksista. Lisäksi tietoaineistoturvallisuudella tarkoitetaan tietoaineiston luokittelua ja sen turvallista käsittelyä ja säilytystä sekä suojataan arkaluonteiset tiedot, tietovarastot ja yksittäiset tiedostot. Perustietoturvatoimenpiteistä huolehtiminen on tärkeää jo senkin takia, että näiden velvoitteiden huolehtimatta jättäminen voi johtaa rikosoikeudelliseen vastuuseen. (Laaksonen & al, 2006, 67; Ruohonen, 2002, 4-5.)

Henkilöstöturvallisuuden tarkoitus on suojata tietojärjestelmä siten, ettei tavallinen käyttäjä toiminnallaan aiheuta riskiä tietojärjestelmälle. Käyttäjän tekemiä tahattomia toimenpiteitä voidaan estää sopivilla koulutuksilla. Käyttäjän tekemiä tahallisia toimenpiteitä tietojärjestelmälle voidaan estää määrittämällä käyttöoikeudet sopivalle tasolle. Valtionhallinnon tietoturvakäsitteistö kuvaa henkilöstöturvallisuutta henkilöstöön kuuluvan tietoturvariskin hallintana henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti – ja käyttöoikeuksien suojaamisen, turvallisuuskoulutuksen ja valvonnan hallinnan osalta. (Henkilöstöturvallisuus, hakupäivä 1.3.2012)

Käyttöturvallisuudella pyritään mahdollisimman turvalliseen käyttöön tietojärjestelmässä ja se liittyy läheisesti henkilöstöturvallisuuteen. Ongelmia syntyy silloin kun tietojärjestelmää käytetään määräysten tai ohjeiden vastaisesti, esimerkiksi käyttämällä heikkoja salasanoja. (Ruohonen 2002, 4-5.)

Käyttöturvallisuuden tavoite on, että koko henkilöstö omaksuu ja hallitsee tietoturvan riittävässä määrin. Tarkoitus on pyrkiä vähentämään tietojenkäsittelystä aiheutuvia riskejä. Yhtenä esimerkkinä käyttöturvallisuudesta voisi olla työkoneen lukitseminen työpisteeltä poistuttaessa. Tällä tavoin estetään ei-toivottujen henkilöiden pääsy tietoihin. Lisäksi tulisi huolehtia, ettei työaseman kiintolevyyn päästäisi kovin helposti käsiksi. Kannettavat tietokoneet ovat pienen ja kevyen kokonsa vuoksi helppo varastaa ja siksi valvontaan tulisi kiinnittää huomiota. Laitteiden käyttö huolimattomasti saattaa aiheuttaa arkaluonteisen tietojen päätymistä vääriin käsiin. Julkisissa liikennevälineissä

kuten junissa ja busseissa tulisi kiinnittää huomiota siihen, ettei vieressä tai takana istuva pääse näkemään salaiseksi luokiteltua tietoa. Puhelimessa puhumistakin on helppo kuunnella jo pelkästään seisomalla tarpeeksi lähellä puhujaa. (Leppänen, 2006, 303-305.)

Tietoliikenneturvallisuudella pyritään suojaamaan niin tietojärjestelmän sisäisessä kuin ulkopuolisessakin verkossa kulkevia viestejä. Tietoliikenneturvallisuutta pyritään parantamaan erottamalla tietojärjestelmän verkko palomuurin avulla muista verkoista. Myös viestien suojaaminen vpn-tekniikalla sekä proxyjen, eli välityspalvelimien avulla. Tietoliikenneturvallisuuden päämäärä on suojata viestintäverkkojen viestiliikenne niin hyvin, että viestit tai tunnistetiedot eivät päädy vääriin käsiin eikä kukaan pääse muokkaamaan, poistamaan tai lisäämään mitään ylimääräistä verkon läpi kulkeviin viesteihin. Jos halutaan päästä edellä kuvattuun tilanteeseen, ainoa vaihtoehto on suojata viestiliikenne tai koko verkko. Verkon suojaamisen haittapuolena on mukana tulevan salausohjelman hallinta sekä myös se, osaako vastaanottaja purkaa tietyllä ohjelmalla lähetetyn viestin. Tietoliikenneturvallisuudella tarkoitetaan myös sitä, että viestintäverkoissa täytyy olla riittävät kiistämättömyys, todentamis- ja pääsynvalvontamenettelyt. Tällöin tunnistamista tai käsittelyä koskeviin tietoihin ei pääse käsiksi kukaan, jolla ei ole valtuuksia niitä käsitellä. (Laaksonen & al, 2006, 67; Ruohonen, 2002, 4-5.)

Fyysisellä tietoturvallisuudella tarkoitetaan turvaa niissä toimitiloissa, joissa tietojärjestelmä sijaitsee. Tietojärjestelmän suojaus krakkereita ja muita tietojärjestelmän sisään yrittäviä henkilöitä vastaan ei tuo lohtua, jos kuka tahansa pystyy halutessaan käyttämään tietojärjestelmän koneita esteettömästi. Krakkeri, päästessään käsiksi yrityksen tietokoneisiin, pääsee lukemaan kaikki ne tiedot joita ei ole kryptattu. Fyysisellä turvallisuudella voidaan tarkoittaa myös rakennusten tilojen ja laitteiden turvaamista erilaisilta uhilta. Kiinteistöhuolto ja vartiointiala vastaa yleensä tämänkaltaisesta fyysisen turvallisuuden ylläpidosta. (Ruohonen, 2002, 4; Hakala, 2006, 11.)

Laitteistoturvallisuudella tarkoitetaan niiden verkon aktiivilaitteitteiden turvallisuutta joista tietojärjestelmä muodostuu, kuten esimerkiksi palomuureja, tietokoneita, johtoja, palvelimia ja reitittimiä. Laitteistoturvallisuudella ja fyysisellä turvallisuudella on paljon yhtäläisyyksiä. Laitteistoturvallisuus koskee myös niitä laitteita jotka sijaitsevat fyysisesti varsinaisen tietojärjestelmän ulkopuolella. Ne tulee sijoittaa niin etteivät ulkopuoliset pääse niihin helposti käsiksi, näin ehkäisten varkauksia, häviämisiä ja muita vahingollisia laitteisiin kohdistuvia tapahtumia, kuten tulipaloilta. (Ruohonen, 2002, 5.)

Laitteistoturvallisuus alkaa jo laitteiden hankinnasta ja päättyy vasta kun laitteistoa ollaan poistamassa. Laitteisto on syytä hankkia mahdollisimman standarisoituneesti, jotta laitteiston päivitys sekä huolto helpottuu ja ne sopivat toisiinsa ja toimivat yhdessä. Laitteiston asianmukainen dokumentointi on myös syytä muistaa. Se helpottaa yritystä pysymään ajan tasalla lisenssi- ja huoltosopimuksissa. Laitteistoturvallisuuteen liittyen yrityksen on syytä myös muistaa tyhjentää käytöstä poistuvien tietokoneiden kovalevyt joko tuhoamalla, päällekirjoittamalla tai tyhjentämällä ne, niin että kovalevyjen tietoja ei pystytä enää hyödyntämään. (Leppänen, 2006, 300-301.)

Laitteistoturvallisuus tarkoittaa myös sitä, että käytetään sellaisia laitteistoja, joista mahdollisesti aiheutuva tietoturvauhka on vähäinen ja että niiden toiminnan kannalta on valittu paras sijainti säilytyksen ja varmuuskopiointien kannalta. (Laaksonen & al, 2007, 67.)

Ohjelmistoturvallisuuden tarkoitus on suojata ohjelmien luvaton käyttö ja varmistaa että ohjelmissa käytettävät lisenssit ovat ajan tasalla. Lisensseillä on merkitystä sekä laittomien ohjelmien estämisessä, että koko tietojärjestelmän kannalta jonkin tärkeän ohjelma mahdollisesti lakatessa toimimasta käyttöajan loppuessa. Ohjelmistoturvallisuus on joukko toimenpiteitä, joilla pyritään suojaamaan tietokoneohjelmia. Tällaisia toimenpiteitä ovat muun muassa: ohjelmiston pääsynvalvonta, ohjelmiston tapahtumatietojen seuranta, tietojen ja ohjelmien varmuuskopiointi, dokumentointi, ohjelmien ylläpito- ja huoltosopimukset ja rekisteröityjen ohjelmien käyttö. Ohjelmistoturvallisuuteen

voidaan vaikuttaa jo käyttöönottovaiheessa, kun asetukset määritellään yrityksen sekä lain vaatimusten mukaan. Esimerkiksi virustorjuntaohjelmiin liittyen on syytä huomioida, että ne tehdään yleensä ulkomailla ja nämä ohjelmat voivat kerätä laittomasti tietoa tietojärjestelmää käyttävistä henkilöistä. (Laaksonen & al, 2007, 67;Ruohonen, 2002, 4-5.)

3 TIETOTURVATYÖ

3.1 Lähtökohdat

Organisaation kokonaisvaltaisen tietoturvallisuuden nostamisprosessin alkaessa yleensä ensimmäinen vaihe on tietoturvakartoitus. Sen tarkoituksena on selvittää oman tai kohdeorganisaation perustiedot ja sen tietojärjestelmien tietoturvallisuuden nykytila. Tietoturvakartoitus on yleensä hyvin yksilöllinen työ ja siten kartoitustyön ratkaisujen täytyy mukautua aina organisaatiokohtaisesti. Kartoituksen tulosten pohjalta voidaan sitten määritellä riskikohteet, tietojen tärkeysjärjestys ja tarvittavat toimenpiteet niiden suojaamiseksi. Tietoturvakartoitus on syytä uusia säännöllisin väliajoin tietoturvatason mittaamiseksi, varsinkin jos tietoturvan suhteen tapahtuu suuria muutoksia. (Simsala Team Oy. Tietoturvakartoitus. Hakupäivä: 31.1.2012.)

Tietoturvakartoituksen tavoite on antaa organisaatiolle ajantasaista tietoa siitä miten yritys on tähän mennessä hoitanut tietoturvansa ja kuinka sen tulisi sitä kehittää jatkossa. Nykytilan analyysin perusteella pystytään selvittämään missä kohdin yritys voisi parantaa toimintaansa. Täydellistä tietoturvaa ei ikinä pystytä saavuttamaan ja se on myös hyvin vaikea määritellä. Vahva tietoturvaprosessi vaatii ympärilleen sekä pitkälle vietyä osaamista, että toimivia tietoturvaratkaisuja (Cygate, Hakupäivä: 15.9.2012). Tämä on haastavaa etenkin, kun on kyse pienemmästä organisaatiosta. Niissä vaadittava tietoturvan taso voidaan määritellä vaikkapa niin, että tietoturvaan liittyvistä onnettomuuksista selviäminen on todennäköistä ja niiden tapahtuminen on epätodennäköistä. Tietoturvan toteuttaminen ja ylläpito voi vaatia paljon resursseja, enemmän kuin pienellä yrityksellä on varaa sijoittaa. Lisäksi toimet voivat tuoda kaikenkokoisia muutoksia yrityksen arkisiin toimiin ja näitä ei ehkä haluta tai voida resurssien takia toteuttaa. Tästä syystä pyritään pääsemään juuri optimaaliseen ja järkevään yrityskohtaisesti määriteltyyn tietoturvaratkaisuun.

Tietoturvallisuuden yleinen tehokkuus varmistetaan valvonnalla. Tietoturvaan liittyvä valvonta ei poikkea mitenkään merkittävästi tavanomaisesta yrityksen johdon suorittamasta valvonnasta, se vain keskittyy enemmän toteutuneiden tietoturvatoimenpiteiden kautta saavutetun suojauksen seuraamiseen. Näin johto voi varmistua tietoturvallisuuden riittävyydestä ja asianmukaisuudesta. Tietoturvan valvonnalla ja seuraamisella on mahdollista kerätä tärkeää tietoa sekä paljastaa mahdollisia tietoturvallisuuteen liittyviä kehityskohteita, kuten erilaisia heikkouksia ja aukkoja tietoturvassa. (Laaksonen & al, 2007, 261.)

Yleinen ja tunnetuin standardi yrityksien tietoturvapolitiikalle on ISO 17799, joka määrittää yleiset ohjeet ja toimintaperiaatteet organisaatioiden tietoturvan hallintatoimien aloittamiseksi, ylläpitämiseksi ja parantamiseksi. Se on pyritty suunnittelemaan soveltuvaksi niin pienten kuin suurtenkin yritysten tietoturvastandardiksi. Sen nimestä selviää, mistä standardissa tarkemmin on kyse. ISO/IEC 1779:2005, jonka kirjaimet ovat lyhenne sanoista Information Technology, Security Techniques, Code Of Practice for Information Security. Standardia ei ole tarkoitettu sertifioinnin koko perustaksi, jolloin se ei yksin riitä tekemään organisaatiosta ISO 17799 -sertifioitua, vaikka organisaatio itseään sellaiseksi kutsuisikin. (Laaksonen & al, 2007, 86.)

ISO 17799 luotiin BS 7799 -standardin pohjalta vuonna 2003 ja siitä on julkaistu uusi versio vuonna 2005. Vuoden 2005 uudistuksessa julkaistiin kokonaan uusi aihealue, nimeltään tietoturvahäiriöiden hallinta eli ”Information Security Incident Management”. Tämän lisäksi osittain koko standardin sisältöä oli muutettu ja aihealueiden nimiä muutettu. Uudessa versiossa on myös korostettu johdon vastuuta ja otettu enemmän huomioon ulkoistuksen vaikutukset tietoturvallisuudelle. Lisäksi standardin luettavuutta on pyritty parantamaan muokkaamalla tekstiä ymmärrettävämpään muotoon. Uudistuksen tarkoitus oli muokata standardia niin, että se vastaisi paremmin nykypäivän toimintaympäristöä -ja järjestelmiä. (Laaksonen & al, 2007, 83-85.)

Sertifikaatteja myönnetään yrityksille auditointien kautta. Auditoinneissa tarkastetaan, että yritys todella toimii ja on kelpoinen saamaan sertifikaatin. Myös auditoinnit järjestetään standardien pohjalta. Näitä ovat BS-7799 ja ISO

27001. Molempien vaateiden täyttymisen perustana toimii ISO 7799 standardin toteutuminen. Koska kyseistä standardia käytetään hyvin oleellisena osana organisaatioiden tietoturvan sertifiointia, on se myös hyvä pohja tietoturvakartoitusta tehdessä. (Laaksonen & al, 2007, 85 & 216.)

Yritys hyötyy monella eri tapaa sertifikaatistaan, sillä sertifikaatti voi esimerkiksi nostaa omistajien ja asiakkaiden luottamusta yrityksen toimintaan. He voivat sertifikaatin nojalla varmistua, että organisaatio pelaa tiettyjen yhteisten sääntöjen mukaan, sen tietoturvallisuus on järjestetty riittävän hyvin ja että se täyttää tietyt laatuvaatimukset. Myös yritysten välisessä kanssakäymisessä sertifikaatit tuovat luotettavuutta toiminnan turvallisuuteen, kun molemmat osapuolet toimivat samalla kaavalla. Joskus toinen osapuoli, asiakas tai toinen yritys, saattaa edellyttää organisaatiolta sertifikaatin omaamista, ja jopa sertifikaattimukaisuuden todistamista yhteisen kanssakäymisen takeeksi. (Laaksonen & al, 2007, 85 & 216.)

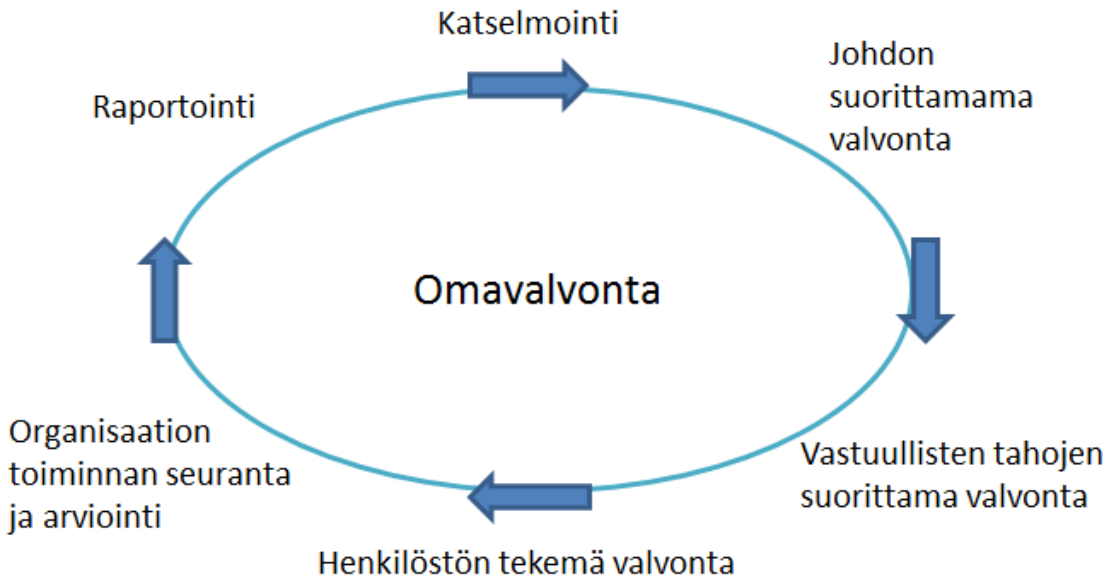
Tietoturvapolitiikka määrittelee ohjeita ja yleisiä toimintaperiaatteita organisaation tietoturvallisuuden hallintatoimen käynnistämiseksi, ylläpitämiseksi ja parantamiseksi. Erilaisten organisaatioiden lähtökohdat tietoturvalle vaihtelevat siinä määrin, ettei mikään yksittäinen tietoturvapolitiikan malli voi soveltua aivan kaikkien käyttöön. Yleisistä standardeista ja ohjeista huolimatta organisaatioissa laaditut tietoturvaa koskevat politiikat ja säädännöt ovat hyvin erilaisia. Erilaisia julkisia palveluita, kuten kunnanvirastoja ja osakeyhtiöitä velvoittavat jo monet julkisuusvelvoitteet, johtuen niille määritellyistä lainsäädännön vaatimuksista. Jo tästä syystä tietoturvapolitiikat vaihtelevat suuresti eri organisaatioiden välillä. (Yrityksen tietoturvapolitiikka, Hakupäivä: 1.4.2012.)

3.2 Tehtävät ja vastuut

Organisaatiossa tapahtuvaa tietoturvallisuuden toteutumisen valvontaa suorittavat useat eri tahot. Esimerkiksi johdon tehtäviin lukeutuvassa sisäisessä tarkastuksessa käsitellään vuosisuunnitelman yhteydessä tietoturvaan liittyvien riskien kartoituksia ja selvityksiä. Valvontaan liittyvät vastuut on jaettu eri puolille organisaatiota tehtäväalueiden pohjalta. Verkon aktiivilaitteiden ja palvelimien tilaa sekä verkossa tapahtuvan liikenteen valvontaa suorittaa tietohallinto. Järjestelmien pääkäyttäjät ja tietojen omistajat valvovat osaltaan tiedon oikeellisuutta. Liiketoimintayksiköissä esimiehet valvovat alaistensa käyttöoikeuksia ja mahdollisesti verkkokäyttäytymistä. Erilaiset tietoturvaorganisaatiot valvovat tietoturvaan liittyvän ohjeistuksen noudattamista ja teknisen tietoturvallisuuden tilaa. Tavallinen työntekijä toimii osaltaan valvojana jokapäiväisen toimintaympäristönsä tietoturvallisuuden saralla ja raportoi eteenpäin esimiehelleen mahdollisia poikkeavuuksia havaitessaan. (Laaksonen & al, 2007, 262.)

Johto järjestää katselmoinnin sekä tietoturvallisuuden arvioinnin säännöllisin väliajoin. Katselmoinnin ei tarvitse olla virallinen, vaan se voi olla epäformaali keskustelutilaisuus ja se voi perustua juurikin organisaatiossa raportoituihin havaintoihin. Yrityksen henkilökunta voi arvioida toimintaansa ja pyrkiä parantamaan sitä omavalvonnan avulla. Omavalvonnalla on merkityksensä ennaltaehkäisevänä vaikuttajana tietoturvallisuuteen liittyvissä uhissa ja asioissa. Omavalvonta rakentuu sovittujen suunnitelmien ja ohjeiden noudattamisesta, raportoinneista, turvallisuuteen vaikuttavien toiminnallisten suunnitelmien laatimisesta sekä riskien arvioinnista. Omavalvonta on jatkuvaa parantavaa toimintaa ja sen tärkein osatekijä on työyhteisön ylläpitämä valvonta. Pitäen sisällään paljon omaehtoista suunnittelua ja toteutusta, omavalvonta on hyvä keino ohjata henkilöstöä kohti yrityksen kannalta oikeaa toimintatapojen noudattamista. (Laaksonen & al, 2007, 261-264.)

Kuvio 1 havainnollistaa omavalvonnan kulkua organisaatiossa tietoturvallisuuden seurannan ja valvonnan osalta. Omavalvonnan toimivuus perustuu siihen, että kaikki osallistuvat siihen, aina henkilöstöstä johtoon saakka. Näin organisaatio itse valvoo tietoturvallisuutensa toimivuuteen vaikuttavia tekijöitä yhdessä vastuullisten tahojen kanssa.



Kuvio 1. Tietoturvallisuuden seurannan ja valvonnan viitekehys. (Laaksonen & al, 2007, 262.)

Organisaation tietoturvan valvonnalla varmistetaan, että esimerkiksi sen tietoturvaohjelma on käytössä ja säännöksiä noudatetaan, samalla ylläpitäen tietoisuutta tietoturvauhista, jotka ovat yrityksen toiminnan kannalta oleellisia. Valvonta voidaan jakaa kahteen osaan, jotka ovat organisaation oman toiminnan valvonta ja ulkopuolisen toimintaympäristön tarkkailu tai valvonta. Organisaation oman toiminnan valvonta koostuu tiedosta, joka on kerätty tietoliikenneverkon, tietojärjestelmien ja loppukäyttäjien toiminnasta. Kyseisistä kerätyistä loki- ja raporttitiedoista ilmenee oikeanlainen ja vääränlainen toiminta, sekä saadaan tietoa havaituista poikkeavuuksista. (Laaksonen & al, 2007, 261-264.)

Valvonnan tulee olla julkista ja täyttää lainsäädännölliset vaatimukset. Henkilöstön tulee saada tietää miten ja minkälaisiin asioihin valvonta kohdistuu. Tietoturvaohjeistuksella on myös psykologinen merkitys: se ohjaa henkilöstöä

toimimaan tietyllä, oikealla tavalla. Organisaation ilmoittaessa minkälaisia menetelmiä tiettyihin kohteisiin on käytetty, henkilöstö tulee paremmin tietoisiksi tärkeistä, turvaamisen arvoisista kohteista. Tietoturvaa koskevien sääntöjen rikkojalle seuraa esimiehen toimittama rangaistus, joka voi ensituntumalta vaikuttaa hiukan äärimmäiseltä, mutta mittavammassa organisaatiossa se voi olla tarpeellista. (Laaksonen & al, 2007, 261-264.)

Palvelimiin ja verkkolaitteisiin tehdään satunnaisia tarkastuksia säännöllisin väliajoin. Näin varmistutaan siitä, että laitteet ovat asetuksineen dokumenttien mukaisia ja järjestelmä on päivitetty. Valvontaa voi suorittaa henkilökunta tai jokin ulkoinen, etukäteen määritelty taho. Valvonnasta voi tiedottaa etukäteen laitteiden ylläpitäjille ja loppukäyttäjille, mutta se ei ole välttämättömyys. (Laaksonen & al, 2007, 263.)

Sisäiseen valvontaan liittyy useita eri osa-alueita:

- Pääsynvalvonta käsittää loogiset ja fyysiset pääsykontrollit.
- Verkkoliikenteen valvontaan sisältyy tietoliikennehäiriöiden, virusten leviämisen, palvelunestohyökkäysten ja tunkeutumisyritysten kontrollointi.
- Käytön valvonta pitää sisällään hallinnollisen valvonnan eli varkaudet, tietovuodot ja erilaiset laiminlyönnit.
- Tekninen valvonta sisältää kapasiteettien riittävyyden tarkkailun, laitteiden rikkoutumiset ja sovellusvirheet sekä tietoturva-aukot.
- Muutoshallintaan kuuluu järjestelmiä ja laitteistoa koskevat muutokset.
- Järjestelmäkehityksessä on muutamia yhteneväisyyksiä muutoshallinnan kanssa, kuten päivityspakettien ja uusien toiminnallisuuksien testauksen ja käyttöönoton valvominen, mutta on muilta osin aivan oma lukunsa.
- Organisaation valvontajärjestelmän tulee myös kattaa muutospyyntöjen oikeellisuuden testaus, sekä muutosten yleinen hallinnoiminen. (Laaksonen & al, 2007, 263.)

Ulkopuolisen toimintaympäristön valvomisella tarkoitetaan jatkuvaa ympäristön tarkkailua tietoturvallisuuden nimissä. Tarkkailtavia asioita ovat esimerkiksi

uudet uhat ja muut turvallisuuteen vaikuttavat tekijät. Tarkkailu voi olla yksinkertaisimmillaan tietoturvauhkista kirjaa pitävien virastojen tiedotteiden ja uutisten lukemista. Myös virustorjuntaohjelmien ja palomuurivalmistajien sivuilta löytää paljon ajankohtaista tietoa tietoturvauhista. (Laaksonen & al, 2007, 265.)

Tietoturvan seuranta on organisaatiossa tapahtuvaa, tietoturvaohjelman mukaista toimintaa ja sen hierarkisesti määriteltyä analysointia. Seuranta on rinnastettavissa auditointiin. Toimiakseen seuranta vaatii erilaisten tietoturvauhkien ja organisaation tietojärjestelmien tuntemusta. Määritelläkseen oman tietojärjestelmänsä tietoturvallisuuden tason organisaatio voi käyttää esimerkiksi ulkopuolista auditointia, mutta voi suorittaa määrittelyn myös itse erilaisten hyväksi havaittujen viitekehysten ja kypsyysmallien avulla. Seuranta on yksinkertaisuudessaan oman tietoturvallisuuden nykytilan ja sille asetettujen tavoitteiden vertailua. Käytännössä tämä jakautuu kahteen osa-alueeseen, jotka ovat hallinnolliseen ja teknisen puolen kehitysehdotukset joiden perusteella organisaatio ohjaa toimintaansa oikeaan suuntaan. (Laaksonen & al, 2007, 265-266.)

Tekninen osa-alue keskittyy organisaation järjestelmän sisältämiin, tiedossa oleviin haavoittuvuuksiin. Haavoittuvuuksia löydetään ajan kuluessa yhä lisää ja organisaatio pystyy oman valvontamekanisminsa ansiosta päivittämään järjestelmänsä ajanmukaiselle, tarvittavalle tasolle. Seuranta tukee tätä mekanismia ja varmistaa sen toimivuuden, edesauttaen organisaation tietoturvan nostoa vastaamaan vaatimuksia. Tällainen haavoittuvuustestaus on silti vain osa organisaation tietoturvan seurantaprosessista. Siihen kuuluu myös muun muassa tietojärjestelmien ja itse tiedon käsittelyyn liittyvien toimintaohjeiden ja toimintatapojen läpikäynti ja niiden noudattamisen varmistaminen. (Laaksonen & al, 2007, 265-266.)

Seurannan tulee olla jatkuva, alati käynnissä oleva prosessi, jotta se toimisi tarkoituksenmukaisella tavalla. Yksi auditointi antaa kuvan vain sillä hetkellä vallitsevasta tilanteesta ja asiat voivat muuttua ajan kuluessa. Keskeinen haaste on varmistaa, että organisaation toiminta todella noudattaa ja tukee annettuja ohjeita, määrityksiä ja tavoitteita. Auditoinnin avulla yritys voi varmistua siitä,

että tietojärjestelmiä käytetään oikein, näin esimerkiksi vapauttaen työntekijöitä eli inhimillisiä resursseja muihin tarpeisiin. (Laaksonen & al, 2007, 265-266.)

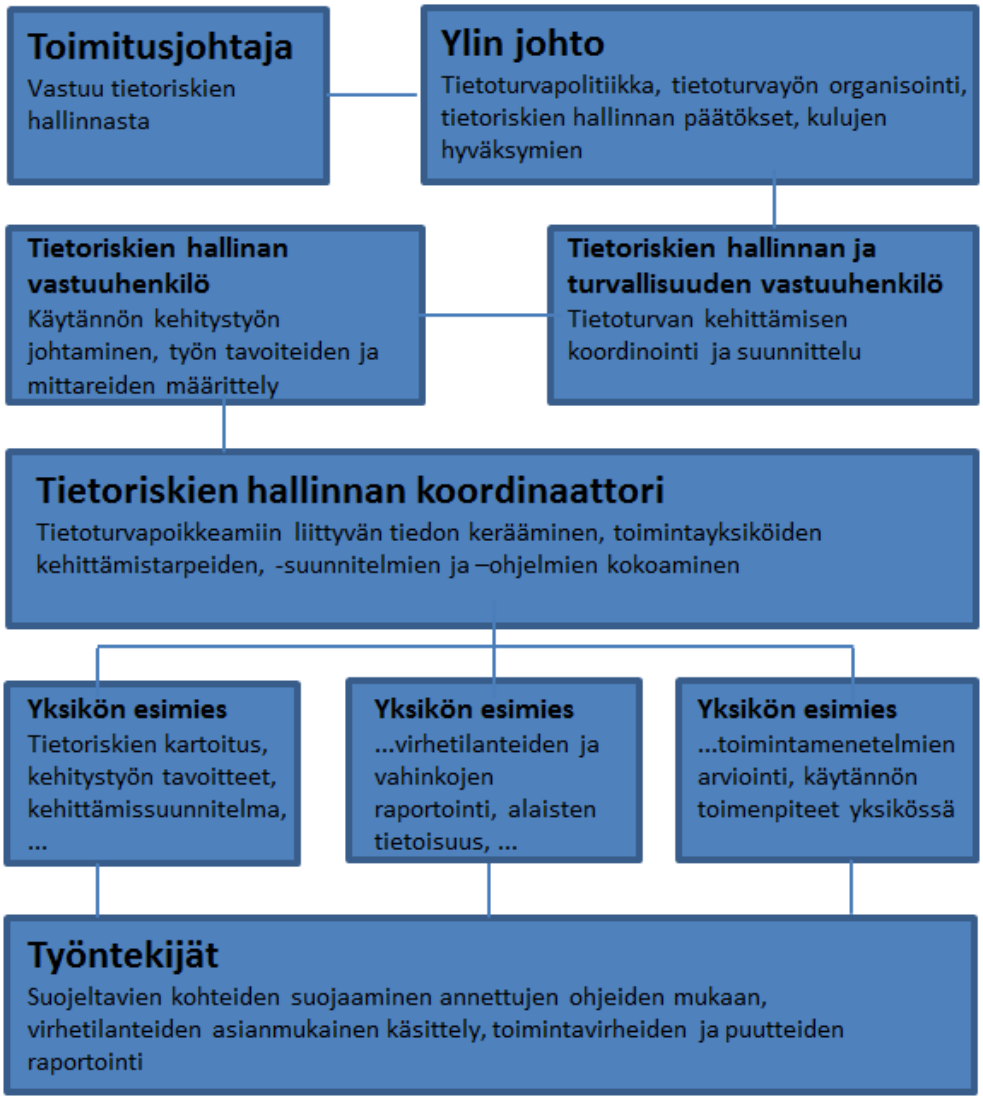
Ylin johto eli organisaation mahdollinen toimitusjohtaja, johtoryhmä ja esimies kantaa suurimman vastuun tietoturvan ylläpidossa ja kehityksessä. Toimitusjohtaja varmistaa tietoturvan pysymisen johdonmukaisena, jotta se pysyy kohdistettuna oikeille osa-alueille. Hän siis vastaa myös tietoturvaan liittyvistä kehityspäätöksistä. Lisäksi toimitusjohtaja vahvistaa tietoturvaan liittyvän politiikan, organisaation ja vastuut. Ylimmän johdon vastuisiin kuuluu organisaation tietoturvapolitiikan luominen ja päivittäminen, sekä tietoturvatyön organisointi. Tehtäviin kuuluu myös myönteisen tietoturvapolitiikan luominen, ja henkilökunnan tietoturvaan liittyvän tietoisuuden lisääminen. Johtoryhmän tehtävänä on myös hyväksyä tietoturvan kulut. Johtoryhmästä valitaan henkilö vastaamaan tietoturva-asioista ja etenkin sen hallinnan edistämiseen liittyvistä seikoista. Tämän vastuuhenkilön ja mahdollisten muiden toimintayksiköiden johtajien raporttien perusteella johtoryhmä tekee päätöksensä tietoturvan kehittämisen suhteen. (Kyrölä, 2001, 234.)

Esimies kantaa vastuun toimintayksikkönsä piirissä. Hän viestii eteenpäin yksikössään raportoiduista virhetilanteista ja niihin kuluneista resursseista tietoturvallisuuden koordinoijalle. Tietoturvan yleinen toiminta ja sen jatkuvuus on esimiehen vastuulla, kuten myös alaisten tietoisuus tietoturvaan liittyvissä käytännöissä ja ohjeissa. Esimies pitää toimintayksikkönsä henkilökunnan tietoisena heidän velvoitteistaan tietoturvan osin, siihen liittyvien käytäntöjen merkityksistä, valvoo että ohjeita ja -tietoturvapolitiikkaa noudatetaan, sekä tiedottaa mahdollisten laiminlyöntien seuraamuksista. Erilaisten toimintamallien riittävyyden arviointi suhteessa kartoitettuihin tietoriskeihin kuuluu esimiehen vastuisiin. (Kyrölä, 2001, 211–217.)

Henkilökunnan ja yksittäisen työntekijän rooli organisaation tietoturvan kehittämisessä on usein hyvin pieni, sillä kehitystyö jää yleensä ylemmälle johdolle ja esimiestasolle. Tulee kuitenkin muistaa, että työntekijä on enemmän tekemisissä jokapäiväisissä käytännön asioissa ja huomaa täten parhaiten varsinaiset puutteet ja muutokset tietoturvallisuuden kannalta. Tämän takia

johdon olisikin syytä kuulla työntekijöitä enemmän tietoturvaa kehittäessä, sillä ilman heidän näkemystään ohjeista ja toimintamalleista saattaa tulla käytännön asioita vaikeuttavia ja hankalia, niiden ehkä ollessa ristiriidassa työtehtävien kanssa. Ristiriitatilanteissa henkilökunta saattaa alkaa karttaa ohjeita ja kiertää suojauksia. (Kyrölä, 2001, 217–221.)

Työntekijöiden ensisijainen vastuu on esille tulleiden virheiden ja puutteiden raportointi eteenpäin esimiehelle, sekä virhetilanteiden asianmukainen hallitseminen. Vastuisiin lukeutuvat myös sekä niin sanottu yleinen huolellisuus, kuten verkkokäyttäytyminen ja muut jokapäiväiset toimet tietoturvan hallinnassa, että omaan tiedon käsittelyyn liittyvien velvollisuuksien sisäistäminen. (Kyrölä, 2001, 217–221.)



Kuvio 2. Tehtävät ja vastuut. (Kyrölä, 2001, 142-145, 208-221, 234-235)

Kuvio 2 kuvastaa organisaation henkilöstön tehtäviä ja vastuita, sekä näiden yhteyksiä toisiinsa. Työntekijät raportoivat ongelmatilanteet yksikkönsä esimiehelle, joka raportoi ne ylöspäin ja niin edelleen. Tällä tavoin esille tulleet ongelmat päätyvät asianmukaisten tahojen tietoon ja ne ratkaistaan oikealla tavalla.

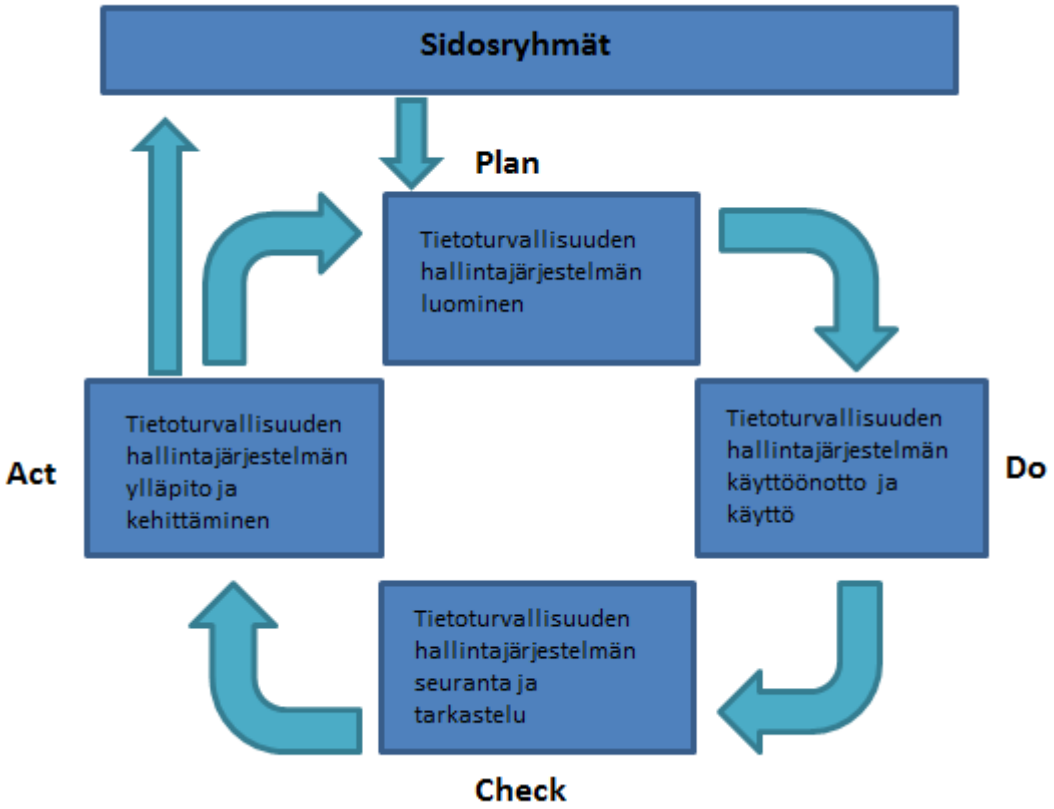
3.3 Tietoturvan prosessi

Tietoturvan parantaminen kuuluisi hoitaa yhtenä, jatkuvana prosessina, joka toteutuu organisaation kaiken muun toiminnan ohessa. Erilliset projektit eivät yleensä toimi, ainakaan pitemmän tähtäimen ratkaisuna käytännön tietoturvassa. Toimintakokonaisuutena kyseinen prosessi on yleensä yksittäisen henkilön vastuulla ja henkilö delegoi sen eri osa-alueiden päätösvaltaa alaisilleen, ollen kuitenkin itse vastuussa prosessista kokonaisuudessaan. Kyseinen vastuuhenkilö tarvitsee riittävästi valtaa ja oikeuksia prosessinsa hallintaan, joten hän on yleensä joku yrityksen johdosta. (Hakala et al., 2006, 20–21.)

Prosessimuotoiset tietoturvaratkaisut toimivat paremmin organisaatioissa, sillä siten tietoturvan vaatima työ saadaan yhdistettyä jokapäiväiseen työhön ja osaksi sitä. Tietoturvan kehittämisen tulisi kuulua organisaation tavoitteisiin jatkuvana, toimintaa tukevana prosessina. Tietoturvan prosessi on hyvin oleellinen osa tietoturvan hallintajärjestelmän käytännön toimia. Hallintajärjestelmällä tarkoitetaan organisaation tietoturvaa kokonaisuudessaan, eli sen eri osia aina tietoturvapolitiikasta yksittäisiin kontrolleihin. Tietoturvan hallintajärjestelmille on määritelty kansainväliset standardit, niiden ollessa tärkeä osa yritysten suojausta. Tunnustetuin ja sertifioiduin näistä on ISO 27001 ja se pääajatus on hallintajärjestelmän pohjautuminen eräänlaisen laatuympyrän mukaiseen prosessiin. (Kyrölä, 2005, 28).

Kuvio 3 havainnollistaa PDCA-kehityssykliä. Aluksi suunnitellaan, sitten tehdään. Näiden vaiheiden jälkeen tulokset tarkistetaan ja tehdään mahdolliset korjaukset (Plan, Do, Check, Act). Sykli on päättymätön prosessi, jossa korjausten jälkeen palataan aina alkuun ja ollaan hieman lähempänä tavoitetta.

Kehitys siis perustuu eräänlaisiin sykleihin, jossa omat tietomme ovat aluksi rajalliset, mutta kehittyvät kierrosten aikana. (Hakala et al., 2006, 49)



Kuvio 2. Hallintaprosessi PDCA-mallin mukaan. (Hakala et al., 2006, 49)

Tietoturvan prosessin aloitukseen kuuluu eri vaiheita. Ensin luodaan toiminnalle suunnitelma, jossa määritellään yrityksen tarpeet ja resurssit. Näiden määrittelemiseen kuuluu vahvana osana riskienhallinta eri osa-alueineen. Aloituksen ensimmäinen varsinainen työvaihe on yleensä tietoturvakartoitus.

3.4 Riskienhallinta

Riskillä tarkoitetaan mahdollista ihmisen tai luonnon aiheuttamaa uhkaa, eli negatiivista lopputulosta, joka liittyy jonkin positiivisen asian tavoitteluun. Se on vahinkoa aiheuttava tapahtuma, joka saattaa toteutua. Uhalla taas on oma tietty numeroarvonsa, joka taas on kyseisen vahingollisen tapahtuman toteutumisen todennäköisyys. Itse vahinko on tapahtuma ja menetys, joka aiheutuu uhan

toteutuessa. Riskin numeerinen suuruus on vahingon odotusarvo. (Virtanen, 2004, 9–13.)

Riskienhallinta tarkoittaa näiden uhkien ja niistä aiheutuvien menetysten hallitsemista organisaation omien ohjeistusten mukaisella tavalla. Riskit tulee määritellä asianmukaisella tavalla. Riskien määrityksiin kuuluu niiden tunnistaminen, analysointi ja arviointi. Riskeistä luodaan luettelo, jossa kuvataan riskit sekä miten analysoitua riskiä käsitellään. Näistä määrittelyistä selviää, mikä on riskin toteutumisen todennäköisyys ja mitkä ovat niiden aiheuttamat jatkotoimet. (Vaarojen tunnistaminen ja riskien arviointi, Hakupäivä 17.3.2012.)

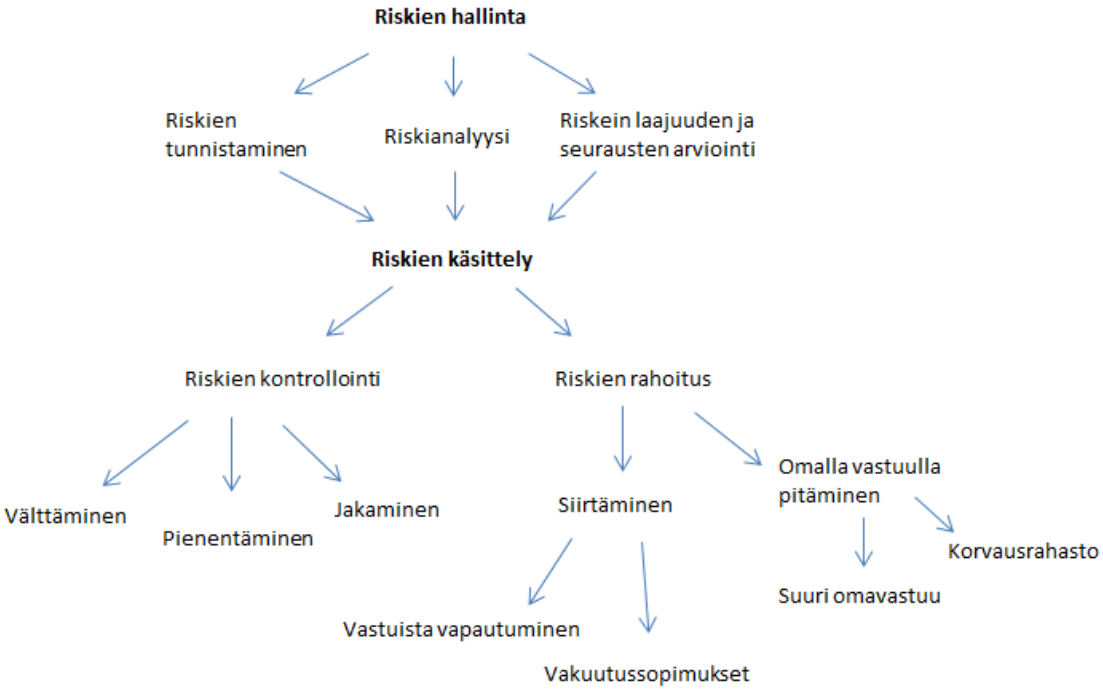
Riskin suuruus määräytyy vahingollisen tapahtuman todennäköisyyden ja sen seurausten mukaan. Määritysten lopputuloksena voidaan tuottaa taulukko, jossa näitä riskin ulottuvuuksia käytetään kuvastamaan riskin suuruutta. Esimerkiksi jos riskin seuraukset ovat vähäiset ja sen todennäköisyys erittäin epätodennäköinen, määrittyy riski merkityksettömäksi. Näin resursseja ei mene hukkaan ja pystytään keskittymään merkittävien riskien ennaltaehkäisemiseen ja niihin varautumiseen. (Vaarojen tunnistaminen ja riskien arviointi, Hakupäivä 17.3.2012.)

Riskienhallinta voidaan jakaa toimenpiteiden osalta kahteen eri osa-alueeseen, joita ovat riskien kontrollointi ja riskien rahoitus. Jälkimmäinen, eli rahoittaminen jakautuu kahteen luokkaan, joista toinen on riskin siirtäminen kolmannen osapuolen vastuulle sopimuksen keinoin ja toinen on riskin pitäminen omalla vastuulla. Kontrolloinnilla taas tarkoitetaan erilaisia riskin kontrollointitapoja. Kontrollointi jakautuu kolmeen luokkaan, jotka ovat välttäminen, pienentäminen ja jakaminen. Välttämisellä vahinkoa pyritään estämään erilaisin keinoin pidättäytymällä riskialttiista toiminnasta, pienentämisellä yritetään pienentää vahingon toteutumisen todennäköisyyttä tai varsinaisten vahinkojen pienentämistä ja hajauttamisella riski pyritään pilkkomaan pienempiin osa-alueisiin ja useisiin itsenäisiin riskikohteisiin. Esimerkiksi jakamalla jokin dokumentti osiin useisiin eri kassakaappeihin voidaan vähentää tiedon luottamuksellisuuden vaarantumisen uhkaa. Riskienhallinnan kustannukset

määräytyvät sen mukaan, kuinka suurta turvallisuuden tasoa ollaan tavoittelemassa. Toisaalta, mitä parempi tietoturva, sitä vähemmän mahdollisia toteutuvia uhkia ja niiden aiheuttamia vahinkoja. Vahinkojen torjuminen tulee yleensä halvemmaksi kuin niiden aiheuttamien tuhojen korjaaminen. (Järvinen, 2001, 45.)

Täydellisen tietoturvan tavoitteleminen ei kuitenkaan ole realistinen tavoite, sillä ylivarautumisesta koituvat kustannukset voivat kasvaa valtaviksi hyötyyn nähden. Lisäksi tiukan tietoturvan mukanaan tuomat ohjeet ja toimet vaikeuttavat organisaation työtä ja siten laskevat kokonaisvaltaista toimintakykyä. Mitä korkeampi organisaation suojelutavoite on, sitä suuremmaksi siis käyvät myös kustannukset. Kun kustannukset ovat tiedossa, voidaan alkaa laskea organisaation odotettuja riskikustannuksia. Tietoturvan taso on optimaalinen silloin, kun näistä muodostuva kokonaiskustannus on pienimmillään. (Suominen, 2003, 114–122.)

Kuva 4 havainnollistaa riskienhallintaprosessia, sen eri vaiheita ja valintoja joita prosessin aikana tehdään. Ensin riskit tunnistetaan, analysoidaan ja niiden laajuus sekä seuraukset arvioidaan. Tästä alkaa riskin konkreettinen käsittely, jolloin käsitellään riskin kontrollointi ja käsittelystä aiheutuvien mahdollisten kulujen kattaminen. Riskin voi eri kontrollimenetelmillä pyrkiä välttämään kokonaan, sen seurauksia voi pienentää ja sen voi jakaa, jotta ongelmantilateessa ei jää ilman tukea. Riski voidaan rahoittaa eri tavoin, esimerkiksi palkkaamalla kolmas osapuoli hoitamaan sitä, näin vapautuen itse vastuista osittain tai kokonaan. Riittävän vakuutussuojan omaava organisaatio voi riskin toteutuessa saada menetyksilleen korvaukset. Riskin omalla vastuulla pitäminen tarkoittaa riskin hyväksymistä. Riskiä ei siis siirretä, vaan se kokonaisuudessaan tai osittain päätetään tietoisesti ottaa ja rahoittaa itse. (Suominen, 2003, 99.)



Kuvio 4. Riskienhallinnan prosessimalli vaiheineen. (Suominen, 2003, 99.)

3.5 Tiedon luokittelu

Kun organisaation tietoaineistoja ryhdytään luokittelemaan, tulee lopputuloksesta käydä ilmi muun muassa kyseisen tiedon paljastumisen seuraukset ja se, kenellä on oikeus päästä tietoon käsiksi ja tarkemmin myös se, kenellä on oikeus muokata ja poistaa tietoa. Luokittelussa tiedot jaetaan ryhmiin, jotka ovat julkinen, sisäinen, luottamuksellinen ja salainen tieto. Luokittelun jälkeen tapahtuva suojausprosessi on selkeämpi, kun tieto on luokiteltu tällä tavalla. Julkisen tiedon paljastumisesta on organisaatiolle vain hyötyä, sisäisestä jonkinasteista harmia, luottamuksellisen ja salaisen tiedon paljastumisesta taas suurempaa vahinkoa organisaatiolle. Pienemmissä yrityksissä sisäisellä ja salaisella tiedolla voidaan tarkoittaa samoja asioita, sillä niissä tietoa ei tarvitse luokitella niin tarkasti kuin suurempien organisaatioiden kohdalla on viisasta. (Tiedon luokittelu. Hakupäivä 1.3.2012.)

Taulukko 1 ja 1.1 havainnollistavat tiedon eri luokat ja niiden paljastumisen seurausten vaikutukset organisaatiolle, sekä kenellä on pääsy mihinkin tietoihin.

Taulukko 1. Tiedon luokittelu. Paljastumisen seuraus. (Tilanteen kartoitus; Esimerkki käsittelyohjeista, Hakupäivä 1.3.2012.)

Luokittelu	**Paljastumisen seuraus**
Julkinen tieto	Hyötyä organisaatiolle
Sisäinen tieto	Ei vaikutusta/Pientä haittaa
Luottamuksellinen tieto	Haittaa organisaatiolle
Salainen tieto	Suurta haittaa organisaatiolle

Taulukko 2. Tiedon luokittelu. Pääsy tietoon. (Tilanteen kartoitus; Esimerkki käsittelyohjeista. Hakupäivä 1.3.2012.)

Luokittelu	**Pääsy tietoon**
Julkinen tieto	Kenellä tahansa
Sisäinen tieto	Henkilökunta / Tietty osasto
Luottamuksellinen tieto	Tiedon käyttäjä tai sen omistaja
Salainen tieto	Tiedon käyttäjä tai sen omistaja

Mitkään järjestelmät tai toiminnot, jotka liittyvät suojattaviin tietoihin, eivät saa aiheuttaa riskejä, joiden toteutuminen on todennäköistä. Järjestelmien tulee olla päivitetty ajan tasalle ja niiden toiminnan kannalta tarpeelliset asetukset tulee olla käytössä. Henkilökunnan täytyy osata tietoturvallinen ajattelutapa ja tietoturvasäännöt sekä ohjeet täytyy olla olemassa. (Tiedon luokittelu, Hakupäivä 1.3.2012.)

3.6 Tietoturvasuunnitelma ja -ohjeistus

Tietoturvasuunnitelman päämääränä on varmistaa että tietojärjestelmän suojaus on järjestetty niin hyvin kuin mahdollista ottaen huomioon siihen kohdistuvat riskit. Tällä tavoin voidaan varmistua tietojärjestelmän turvallisuudesta ja varmistetaan, että tietoturvaan käytettävät resurssit eivät ole ylimitoitettuja. Ensimmäinen asia tietoturvasuunnitelmassa on määrittää mitä tavoitteita tietojärjestelmän pitäisi täyttää. Tässä vaiheessa määritellään minkä tasoisena palvelu halutaan ja mitä riskejä tietojärjestelmän käyttäjä hyväksyy. Myös kustannusten maksimitaso voidaan mainita tässä vaiheessa. (Ruohonen, 2002, 6-7.)

Mitä tärkeämmästä järjestelmästä on kyse, sitä paremmin se pitäisi suojata. Yritys voi esimerkiksi hyväksyä sen riskin että yrityksen web-sivulle pystytään ehkä murtautumaan mutta yrityksen toiminnan kannalta oleellisemmat tietojärjestelmän osat kuten esimerkiksi tietokantapalvelin ovat paremmin suojattuja. Käytännössä voidaan siis priorisoida tietojärjestelmän osia tärkeyden mukaan. Tietoturvasta aiheutuvat kustannukset eivät saisi koskaan ylittää niitä kustannuksia, jotka aiheutuisivat jos tietoturvaan kohdistuva riski realisoituisi. Tietoturvan tavoitteet tulisi asettaa sellaiselle tasolle, jonka saavuttaminen on mahdollista. Mahdottomien tavoitteiden asettaminen saattaa luoda virheellisen kuvan järjestelmän laatijoille sen turvallisuudesta, jonka lisäksi järjestelmän ylläpitäjät saattavat turhautua tai tietojärjestelmän suunnitelman uskottavuus voi kärsiä. (Ruohonen, 2002, 6-7.)

Tietojärjestelmä tulee suojata siten, että se koostuu useasta eri tietoturvakerroksesta. Näin vältytään tilanteelta, jossa tunkeutujan tulee läpäistä vain yksi tietoturvakerros, päästäkseen käsiksi kaikkiin yrityksen tietoihin. Tällaisella suojauksella tarkoitetaan esimerkiksi palvelimelle menevän liikenteen seuraamista palomuurin lisäksi myös erillisellä IDS-järjestelmällä. Tietojärjestelmistä puhuttaessa on syytä tiedostaa myös se, että on olemassa muitakin uhkia kuin yrityksen ulkopuolelta tulevat hyökkäykset. (Ruohonen, 2002, 6-7.)

Yrityksen kannattaa luoda erillinen dokumentti, josta selviää täsmällisesti käytössä olevat tietoturvaratkaisut. Kirjattavia asioita ovat esimerkiksi IT-järjestelmien suojamekanismit. Kyseisiä tietoja sisältävää asiakirjaa voidaan kutsua nimellä tietoturvasuunnitelma. Nimitys on kuitenkin harhaanjohtava, sillä dokumentti kuvaa nykyisiä tietoturvan ylläpitämiseksi tehtyjä teknisiä ja hallinnollisia toimenpiteitä. Parempi nimitys on esimerkiksi VAHTI -työryhmän käyttämä tietoturvakäytännöt ja –periaatteet. Varsinainen suunnitelmaosa voidaan nimetä tietoturvan kehittämissuunnitelmaksi. (Tietoturvasuunnitelma 2007, Hakupäivä 15.9.2012.)

Järjestelmällinen johtaminen on avainasemassa silloin kun on tarkoitus luoda yritykselle hyvä tietoturvan taso. Tason kehittämiseen pyrittäessä keskeiseksi asiaksi nousee tietoturvaohjelma, joka käsittää koko yrityksessä luodun ja jo olemassa olevan politiikan sekä ohjeistuksen. Yleensä ohjeistus on luotu jonkun tietyn toimenpiteen suorittamiseksi ja tämä ohjeistus tyypillisesti täyttää tietyt vaatimukset jotka liittyvät standardeihin tai viitekehykseen. Vaatimukset taas on esitelty yrityksen tietoturvapolitiikassa. Seuraavat kolme asiaa luovat perustan yrityksen tietoturvaohjeistuksen tasoille:

1. Politiikka määrittelee yritysjohdon myöntämät resurssit, joilla tietoturvallisuuden puitteet linjaukset ja vastuut yrityksessä hoidetaan.

2. Standardit kuvaavat toimintatapoja, joilla yritys hoitaa tietoturvan toteutuksen käytännössä. Standardilla voidaan tarkoittaa muutakin kuin kansanvälisiä tietoturvastandardeja, kuten esimerkiksi yrityksen omia vakioituja tapoja hoitaa tietyt asiat.

3. Toimintaohjeet luovat selkärangan organisaation tapaan hoitaa tietoturva-asiat. (Laaksonen et al, 2006, 145)

Tietoturvaohjeita laadittaessa täytyy olla selkeä visio siitä miksi ohjeet on ylipäätään luotu. Sen jälkeen kun yrityksen johto, tietoturvallisuusorganisaatio ja muut asian kannalta tärkeät tahot ovat antaneet mielipiteensä ja tietoturvariskit yrityksessä on kartoitettu, on aika luoda tietoturvaohjelma. Ohjelman tarkoitus

on esittää periaatteet, joihin yrityksen tietoturvan käytännön toimenpiteet perustuvat. Ohjelman tarkoitus on selvittää mitä voidaan tehdä tietoturvan tehostamiseksi ja mitä toimenpiteitä se vaatii. (Laaksonen et al, 2006, 145.)

Tietoturvaohjelman tavoite on välttää ongelmien syntyminen. Esimerkiksi yrityksen henkilökunnan tietojenkäsittely, Internet-selailu, sähköpostin käyttäminen, sekä laitteiden ja järjestelmien käyttö edellyttävät ohjeistusta. Tietoturvaohjeistusta sekä teknistä tietoturvaa tulisi kehittää yhtä aikaa. Pelkän teknisen tietoturvan parantaminen ei poista tietoturvaongelmia. Ohjeistus auttaa ottamaan hankituista teknisistä välineistä täyden hyödyn. Selkeä ohjeistus ja ristiriitaisten tietojen välttäminen tukee ajatusta minimoida sekä yhdistää ohjeistusta mahdollisimman paljon tuottaakseen parhaan mahdollisen lopputuloksen. Kun ohjeita käytännössä viedään toteutettavaksi, on selkeä vastuun määrittäminen olennaista. On oltava selkeä tieto siitä mikä asia on kenenkin huolehdittavana. (Laaksonen et al, 2006, 146.)

Tietoturvatoimenpiteillä turvataan yksilön, yhteisön ja yhteiskunnan etuja. Tietoturvallisuus on yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys, sillä yhteiskunnan toiminnot ovat nykyään suurelta osin riippuvaisia tietojen käsittelystä ja siirrosta. Nykyaikaisessa verkottuneessa toimintaympäristössä harva organisaatio on vastuussa pelkästään oman tietoturvallisuutensa tilasta. (Henkilöstön tietoturvaohje 2006, hakupäivä 13.5.2012.)

Suurimmat tietoturvallisuudessa ilmenevät ongelmat johtuvat usein kiireestä, huolimattomuudesta, osaamattomuudesta ja muista tietojärjestelmien toteutuksen ja käytön laadullisista tekijöistä. Tietoturvallisuudesta huolehtiminen on jokaisen organisaatiossa työskentelevän velvollisuus. Tietoturvallisuus on ”juuri niin hyvä kuin sen heikoin lenkki”. Kyse on siis paitsi tekniikasta, myös jokapäiväisistä toimintatavoistamme ja asenteistamme. Puutteellinen tietoturvallisuus vaarantaa valtion, kansalaisten, yhteisöjen ja asiakkaiden edun ja aiheuttaa lisätyötä ja -kustannuksia. Tietoturvallisuutta kehittämällä parannetaan toimintojen luotettavuutta ja jatkuvuutta. (Henkilöstön tietoturvaohje 2006, hakupäivä 13.5.2012.)

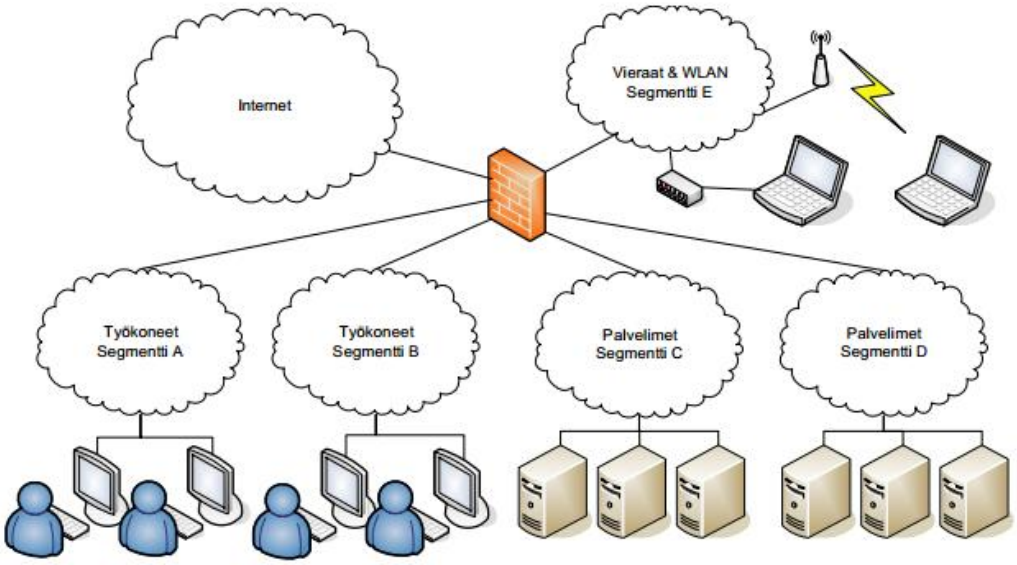
3.7 Tietoverkon infrastruktuuri

Tietoliikenneverkot muodostuvat tietokoneista ja niitä yhdistävistä erilaisista tietoliikenneyhteyksistä, jotka mahdollistavat datan liikkumisen koneiden välillä. Uhkina tietoverkoissa tietoturvan näkökulmasta ovat luvaton tunkeutuminen, siitä mahdollisena seurauksena salakuuntelu ja liikkuvan informaation väärentäminen. Nykyaikana yritystoimintaa ja etenkin sen tietojenkäsittelyä on hyvin vaikeaa toteuttaa ilman kanssakäymistä tietoverkkojen kanssa ja esimerkiksi erilaisia Internetiin perustuvia palveluita tuottavassa yrityksessä tällainen olisi mahdotonta. Tästä syystä tietoverkot tulee suojata asianmukaisella tavalla ja ottaa ne huomioon elintärkeänä osana tietoturvan toteutusta suunnitellessa. Tietoverkon infrastruktuuri tulee suunnitella niin, ettei siihen pääse syntymään yhteydellisiä ”pullonkauloja” ja että se on suunniteltu tiedon saavutettavuuden kannalta oleellisella tavalla. Kaikkein alttiimpia tietoverkoista kumpuaville hyökkäyksille ovat siihen kytketyt palvelin- ja työkoneet, verrattuna esimerkiksi sellaisiin koneisiin joihin täytyy päästä konkreettiseen käsiksi tunkeutuakseen niihin. Tästä syystä hyökkäyksille alttiit laitteet tulee suojata hyvin kyseisiä uhkia vastaan. (Schneier, 2004, 176.)

Palomuuri on työkalu, jolla suojataan verkkoja ja evätään asiattomien henkilöiden pääsy siihen ja sen tarjoamiin palveluihin. Kun verkkoja lähdetään kytkemään toisiinsa, voi kuka tahansa toiseen verkkoon pääsevä liikennöidä myös siihen liitettyyn verkkoon. Tätä liikennettä onkin voitava säädellä, jotta yksityiset verkot voidaan suojata vastaavista julkisista verkoista tulevilta uhilta. Useimmat palomuurit tarjoavat uskottavan suojan tavallisimpia verkkohyökkäyksiä vastaan ja sen yhteydessä voi myös toteuttaa erilaisia verkkovalvontaa tarjoavia toimintoja. Palomuurit toimivat verkon rajoilla, suodattaen vain niiden läpi kulkevia yhteyksiä, joten ne eivät suojaa verkon sisältä tulevia taikka tavalla tai toisella palomuurin ohittavia hyökkäyksiä vastaan. Myöskään sovellustasolla tapahtuvat hyökkäykset, kuten virukset ja muut haittaohjelmat eivät useimmissa tapauksissa kuulu palomuurin suojauksen piiriin. (Schneier, 2004, 189.)

Verkkojen välinen, kumpaankin suuntaan kulkeva liikenne joutuu kulkemaan palomuurin lävitse. Palomuuriin toimii suodattimena ja siihen tehdyt asetukset ja säännöt määrittelevät mikä liikenne pääsee lävitse ja mikä taas estetään. Tämä voidaan toteuttaa verkon eri kerroksilla ja palomuuri voi suodattaa liikennettä sen sisällön perusteella, esimerkiksi IP-otsaketietojen tai estää HTTP-paketeista tunnettuja turvallisuusaukkoja hyväksikäyttävät murtoyritykset. Sovelluspalomuuri toimii sovellustasolla. (Stallings, 2006, 622.)

Lisäsuojan takaamiseksi palomuureja tulisi käyttää julkiselta verkolta suojautumisen lisäksi myös muiden hallinnoimiin yksityisverkkoihin liityttäessä. Suositeltavaa on myös rajoittaa organisaation oman yksityisen verkon sisäisten työ –ja palvelinkoneiden toiminta omiin segmentteihinsä käyttöryhmien perusteella. Tällä tavalla kaikki yhteydet pysyvät järjestelmällisesti hallinnassa, kun segmenttien välistä liikennettä voidaan säädellä halutulla tavalla ja muun muassa väärinkäytösten riski pienenee. Segmenttejä voidaan muodostaa verkon fyysistä infrastruktuuria muokkaamalla, tai virtuaalisesti muodostamalla segmenttejä muun muassa reitittimien ja kytkimien asetuksia hyödyntämällä. Reitittimiä tarvitaan aina verkkoja yhdistäessä, jotta verkkojen välinen liikenne toimii. Reitittimillä voidaan useimmiten suodattaa liikennettä, aivan kuten palomuurillakin, mutta vain sillä verkkokerroksella, jolla se on käytössä. Lisäksi tämä tulee tehdä reitittimen suorituskyvyn puitteissa, joten kovin suurta estolistaa ei kannata reitittimen vastuulle antaa. (Hakala et al., 2006, 185.)



Kuvio 5. Tietoverkon infrastruktuurin malli.

Kuvio 5 havainnollistaa verkkoinfrastruktuuria. Keskellä oleva tiiliseinä havainnollistaa käytössä olevaa palomuuria, joka toimii internetin ja laitteiston välissä. Sen kautta kulkee kaikki liikenne ja haitalliset yhteydet estetään.

WLAN-verkko eli langaton verkko, on oivallinen tapa mahdollistaa työskentely kannettavilla tietokoneilla työtiloissa. Lisäksi se on erinomainen keino tarjota Internet-yhteys organisaation vieraille, riippuen tietenkin organisaatiosta. WLAN-verkot ovat toisaalta liian helposti ei-toivottujen vieraiden tavoitettavissa ja niiden suojaukset ovat yleensä melko heikkoja. Tästä esimerkkinä WEP, joka on purettavissa ”kotikonstein”. Siksipä organisaation tulisi langattoman verkon salauksessaan käyttää vahvempia suojauksia, kuten WPA2- taikka WLAN-riippumattomia VPN-ja SSL -yhteyksiä. Langaton verkko kannattaa myös kokonaisuudessaan eristää yrityksen yksityisestä verkosta, sillä vieraita ei ole viisasta päästää siihen käsiksi. Langattomat lähiverkot eivät ole suositeltava tapa myöskään suojeltaviin verkkoihin liittymiseen. Omien työntekijöiden tarvitsema langaton yhteys voidaan järjestää ulkopuolisesta verkosta kuten muutkin etäyhteydet. (Hakala et al., 2006, 295–296)

3.8 Tietoverkkojen ja -aineistojen suojaaminen

Riskienhallinnassa käytyjen kartoittavien toimenpiteiden, eli tiedon selvittämisen ja luokittelun jälkeen siirrytään suojaaviin toimiin. Eli kun päätökset havaittujen riskien suhteen on tehty ja tarvittava tietoturvataso määritelty, ryhdytään selvittelemään nykyisen tietoturvan puutteita ja paikkaamaan niitä. Tässä vaiheessa päätetään suojausten muoto sekä kontrollit ja ne otetaan käyttöön. Tietoturvan kontrollit ovat mekanismeja tai keinoja, joilla parannetaan esimerkiksi käyttäjän ja laitteiden välistä kanssakäymistä. (Internet verkon käyttötavat ja niiden tietoturvallinen toteutus 2009. Hakupäivä: 15.9.2012.)

Kun tietoverkkoja lähdetään suojaamaan, pyritään yleensä parantamaan tiedon luottamuksellisuutta ja eheyttä sekä estämään erilaisten tietoverkkojen luvaton käyttö. Tietoliikenteen suojaus on hyvin olennainen osa nykyaikaisen tietojenkäsittelyn tietoturvaa, sillä suuri määrä tietoa liikkuu paikasta toiseen aina kun tietoa käsitellään, niin julkisissa kuin yksityisissäkin verkoissa. Liikkuvan tiedon tulee olla siis hyvin suojattu matkan eri vaiheissa. Yksityisen verkon suojaaminen julkisesta verkosta tulevilta hyökkäyksiltä tulee vaatimaan veronsa organisaation resursseista, mutta se on hyvin kannattavaa, sillä käytännön syistä yksityinen verkko yhdistetään julkiseen verkkoon lähes aina. (Internet verkon käyttötavat ja niiden tietoturvallinen toteutus 2009, Hakupäivä: 15.9.2012.)

Organisaation toiminnan jatkuvuuden takaamiseksi on hyvin tärkeää, että tieto on suojattu eikä häviä suurienkaan virheiden ja vahinkojen sattuessa. Varsinkin nykyisissä yrityksissä, tietojenkäsittelyn ollessa erittäin tärkeässä asemassa tämä voidaan nähdä jopa elinehtona. Tiedon varmuuskopiointi ja varajärjestelmät ovat eräitä suojaavia keinoja, jotka oikealla tavalla toteutettuina varmistavat tiedon säilymisen vakavien vahinkoa aiheuttavien tapahtumien toteutuessa. (Internet verkon käyttötavat ja niiden tietoturvallinen toteutus 2009, Hakupäivä: 15.9.2012.)

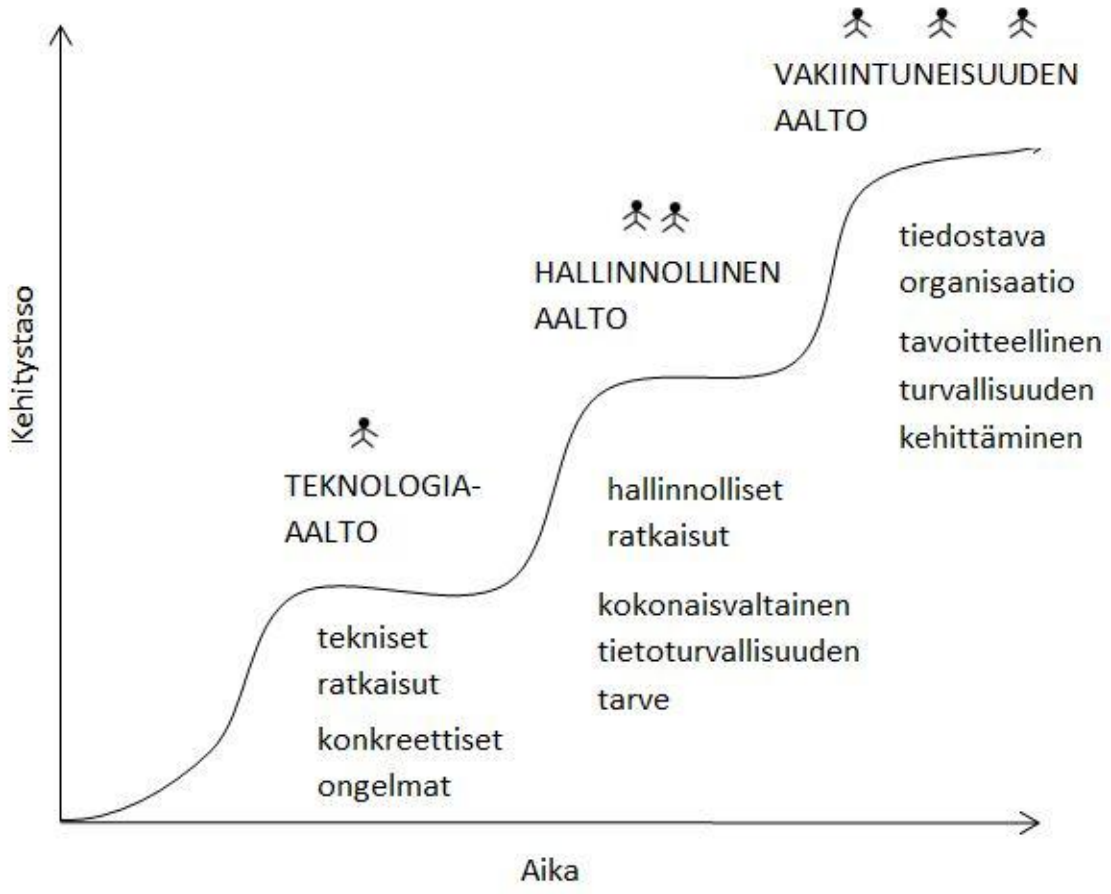
4 KOHDEYRITYKSEN NYKYTILA

Tietoturvakartoituksen tiedonkeruu tapahtui sekä haastattelemalla (Kts. Liite 2) kohdeyrityksen tietoturvavastaavaa, sekä myös yleisten havaintojen kautta. Kohdeyritys on jakautunut neljään eri toimipisteeseen, joista Oulun yksikkö oli tietoturvatyömme kohteena. Toimipisteessä on työntekijöitä noin 20 ja työasemia saman verran, jäljelle jäävissä toimipisteissä henkilökuntaa on vain muutaman henkilön verran. Organisaatiorakenne on jakautunut kahteen, tuotanto- ja toimistohenkilöiden puoleen. Toimistohenkilöiden työnkuvat liittyvät mm. myyntiin ja markkinointiin.

Yritystä lähemmin tarkasteltuna vaikuttaa siltä, että kohdeorganisaation tietoturvaratkaisut ja toimintamallit ovat syntyneet yleisen tarpeen vaatiessa, ilman sen suurempaa järjestäytynyttä suunnitteluprosessia ennen varsinaista toimeen ryhtymistä. Kullakin toimipisteellä on omat toisistaan riippumattomat palomuuri- ja yhteysratkaisut, jotka on korkeintaan kilpailutettu palveluntarjoajien välillä. Näistä on valittu huokein tarjous, jonka on parhaiten katsottu palvelevan oman toiminnan tarpeita. Myös tietoturvan kontrollit on valittu sen perusteella, mitä työntekijät ovat katsoneet toiminnan kannalta tarpeellisiksi.

Kyseisestä toimintatavasta johtuen varsinainen tietoturvatyö voi olla kohdistettu hieman ongelmallisesti, kun resurssit käytetään yksipuolisesti jonkin tietyn tarpeen täyttämiseen. Se ei välttämättä ole tarpeellista oikean akuutin ongelman piileskellessä muualla. Vaikkakin kohdeyrityksessä tiedostetaan tietoturvallisuuden tärkeys ja tarve, sen tietoturvallisuuden kehitystyö on jäänyt selvästi tätä mittaavalla taulukolla teknologia-aallon vaiheeseen. Hallinnollinen puoli on jäänyt vähemmälle. Seuraavan sivun kuviossa 8 asiasta tarkemmin.

Kuva 8 havainnollistaa teknologia-aallon kolmea eri vaihetta. Ensimmäisessä vaiheessa aikaa on kulunut vähiten ja kehitystaso on alhaisin. Kohdeorganisaatiomme on selkeästi kuvion ensimmäisessä vaiheessa, jossa toimintamallit ovat tarvekeskeisiä ja tietoturva on hoidettu pelkillä teknologisilla ratkaisuilla. Kuitenkin jo tässä vaiheessa on huomattu, että tietoturvan hallinnoinnin täytyy tulla mukaan jossain vaiheessa. Tätä seuraavat aallot kuvaavatkin juuri tämän puolen kehittymistä.



Kuva 8. Teknologia-aallot. (Von Solms, Information Security – The Third Wave. 615-620. 2000.)

Kohdeorganisaation toimipiste johon kartoituksemme pääasiassa keskittyy on pienehkö, eikä sen toiminnan pääpaino ole tietojenkäsittelyssä. Tästä syystä sen tietoturvallisuuteen ei ole sen järjestäytyneemmin panostettu esimerkiksi virallisten toimintaohjeiden ja dokumentoinnin muodossa. Tästä huolimatta jokapäiväiset toimet ja muut tietourvallisuuteen liittyvät perusasiat on hoidettu hyvin. Myös erikoistapauksiin on varauduttu ainakin ajatustasolla, jotta niiden mahdollisesti sattuessa kohdalle yksikön toiminta ei lakkaisi. Esimerkkinä tästä organisaatio on keskittänyt toimipisteensä työtilojen työkoneiden ja muiden tarpeiden hankinnat pienille yrityksille, joiden kanssa sillä on historia ja aiempi, pitkä yhteistyö. Toimijat tuntevat toisensa usein henkilökohtaisesti. Tällöin ongelmatilanteissa yritys voi soittaa suoraan tietylle toimijalle ja ongelmat hoidetaan yhteisymmärryksessä.

Kuten todettu, kohdeorganisaation hallinnollinen puoli on puutteellinen. Tietoturvan vastuut on jaettu jonkinlaisesti, mutta tietoturvatyön organisointi, suunnittelu ja dokumentointi on puutteellista. Perustavanlaatuiset tietoverkkojen rakenteita ja topologiaa kuvaavat kaaviot löytyivät kansion pohjalta etsinnän tuloksena, mutta muuten dokumentaatio puuttui. Muun muassa liiketoiminnan vaatimukset tietoturvallisuudelle, sekä organisaation tietoturvapolitiikka ovat kokonaan määrittelemättä. Tästä syystä tietoturvallisuuteen liittyvä kehitystoiminta pohjautuu työntekijöiden aloitteellisuuteen ja toimintaan. Esimerkiksi juuri edellä mainittu suunniteltu siirtyminen toisen operaattorin asiakkaaksi johtui pääasiassa hitaista yhteyksistä ja muista käytännön seikoista, mikä kuvastaa juuri organisaation tarvepainotteista toimintaa. Tämä on selitettävissä juuri organisaation toimipisteen pienuuden ja sen toiminnan painopisteen vuoksi. Parantaakseen tietoturvallisuutensa tasoa kohdeyrityksen tulisi siis panostaa tietoturvan hallinnolliseen puoleen.

Kohdeorganisaation henkilökunta koostuu ammattinimikkeiltään kirjavasta joukosta, mutta siitä puuttuu tietojenkäsittelyn ja tietotekniikan ammattilaiset. Tämän lisäksi yrityksessä on tällä hetkellä vain yksi henkilö, joka hoitaa oman työnsä ohella järjestelmätukea ja muita siihen liittyviä asioita. Tämä muodostaa yritykselle vakavan riskin esimerkiksi sairastapauksen sattuessa, kun muut eivät

osaa suorittaa kyseisiä tehtäviä joko ollenkaan, tai ilman tämän henkilön avustusta.

Yrityksellä ei ole tällä hetkellä myöskään mitään julkista ohjeistusta kuinka tietokoneella työskennellessä tulisi huomioida tietoturvallinen työtapa ja miten ongelmatilanteissa tulisi toimia. Kirjallisen ohjeistuksen puuttuessa on ymmärrettävää, ettei henkilökunta toimi tietoturvallisesti, vaikka heitä kuinka asiassa kouluttaisi. Koulutus unohtuu helposti, mutta ohjeiden avulla muistaminen helpottuisi. Ohjeiden puutteen ja raportin alussa mainitun sopimuksen takia teimme yritykselle yleisiksi ohjeiksi A4–paperiliuskan tietoturvallisista työtavoista työpisteellä. Ohjeissa käsitellään mm. ”puhtaan pöydän” periaatetta, USB-muistitikkujen käyttöä ja salasanojen säilytystä.

Kartoittaessamme yrityksen työasemien virustorjuntaa kävi myös selväksi, että yrityksellä ei ole yhteistä ideaa siitä kuinka asia tulisi hoitaa. Kaikista koneista löytyy jonkinlainen virustorjuntaohjelma, mutta ohjelmien joukko on kirjava. Organisaation varmuuskopiointi on myös puutteellista. Tärkeimmistä tiedoista varmuuskopiot otetaan työpaikalla olevalle verkkokovalevylle mutta työasemien varmuuskopiointia ei ole tällä hetkellä määritetty. Tietoaineistoturvallisuudessa oli myös puutteita. Kohdeorganisaatiolla ei ole minkäänlaista yleistä tiedon ja laitteiston elinkaareen liittyvää käytäntöä, eikä ohjeistusta suojattavien kohteiden tunnistamiseen tai luetteloimiseen, saati niiden omistajien määrittelemiseen ja tiedon luokittelemiseen.

Eräs kehittämisen kohde on kohdeorganisaation salasanapolitiikka. Henkilöstön haastattelusta kävi ilmi puutteellisen tietoturvapolitiikan ohessa myös akuutti salasanapolitiikan puute. Henkilökuntaa ei ole ohjeistettu tai opastettu salasanajärjestelyissä, eli niiden käytössä, muodostamisessa ja vaihdossa. Tästä syystä yrityksessä on muodostunut ns. huono salasanakulttuuri, koska salasanoja ei vaihdeta tarpeeksi usein, ne ovat muodostettu huonon tavan mukaisesti liian helpoiksi ja samaa salasanaa saatetaan käyttää useassa eri yhteydessä. Käytännössä riskit ovat suuremmat niillä henkilöillä kohdeorganisaatiossa, jotka käsittelevät elintärkeitä tietoja kuten tilauksia. Myös

hallintoryhmään kuuluvat henkilöt luovat salasanojen paljastuessa riskin laajempien käyttöoikeuksiensa kautta.

4.1 Tietoturvan nykytila

Yrityksellä on useita toimipisteitä, jotka sijaitsevat ympäri Suomea. Näistä toimipisteistä yhteistyötä teemme Oulussa sijaitsevan toimipisteen kanssa ja tietoturvakartoituksemme keskittyykin lähinnä sen toiminnan suojaamiseen. Ennen toimipisteillä oli sopimukset valtakunnallisen operaattorin kanssa, mutta yhteydet ovat tässä osoittautuneet liian hitaiksi. Lisäksi jokaisella toimipisteellä on oma erinäinen palomuurinsa ja esimerkiksi Oulun toimipisteen palomuurista on vastuussa pieni yhden miehen yritys ja tästä syystä yritys lähti etsimään ratkaisuksi yhtenäisempää kokonaisuutta. Eri sopimusmalleista lähdettiin neuvottelemaan kokouksessa, jossa olimme läsnä. Kuviossa 6 on esitetty yksi esimerkki ratkaisu jolla yrityksen tietoverkkoinfastruktuuri voitaisiin rakentaa.

Kokouksessa kävi ilmi yrityksen nykyinen tietoturvan tila. Palomuuri on vanhanaikainen sekä sen ylläpito ongelmallista, koska se on yhden ihmisen vastuulla. Nämä seikat huomioon ottaen sitten lähdettiin valitsemaan sopivinta sopimusmallia. Lähimmäksi pääsi valtakunnallisen operaattorin tarjoama yritysverkkoratkaisu, koska se on edistyneempi ja palveluiltaan monipuolisempi. Kyseiseen ratkaisuun pystyy valitsemaan lisää palveluita tarpeen tullen, joten se skaalautuisi asiakkaan tarpeisiin sopivaksi. Kohdeyrityksen toimipisteiden käyttäjämäärä on noin 25, valtaosan kuitenkin sijaitessa Oulussa. Koska suurin osa käyttäjistä on Oulun toimipisteessä, tulisi sinne kohdentaa enemmän verkkokapasiteettia kuin muihin toimipisteisiin. Operaattorin puolelta erilaisia lisäpalveluita esitettiin useita, mutta niiden ei katsottu olevan tarpeellisia. Tulevan palvelun toivottiin olevan realistinen ja toimiva kokonaisuus, johon ei sisältyisi liikaa erilaisia ominaisuuksia, joita ei lopulta edes käytettäisi.

4.2 Kehityssuunnitelma

Kehityssuunnitelman pääasiallinen tarkoitus on ehdottaa yritykselle sen toiminnan kannalta järkevimmin skaalautuva ratkaisu tietoturvan toimivuuden kannalta. Merkittävin asia, joka kartoitusta laatiessa nousi esille oli dokumentoinnin puute tietoturvaan ja sen eri osa-alueisiin liittyen. Kohdeorganisaatiolla tietoturvatyö on ruohonjuuritasolla ja heidän puutteisiinsa lukeutuu tietoturvapolitiikka, -suunnitelma ja siihen liittyvät ohjeistukset**.** Organisaation toiminnan pääpaino ei ole tietojenkäsittelyssä eikä yrityksessä ole välttämättä ollut ymmärrystä kuinka tärkeässä asemassa tietoturva on nykypäivän yhteiskunnassa, siksi se tarvitsisi silti selkeän suunnan tietoturvalleen. Nämä saataisiin kehittämällä organisaatiolle juurikin edellä mainittu tietoturvapolitiikka ja siihen liittyvät dokumentaatiot, joista käy ilmi organisaatiossa tehtävä tietoturvatyö sekä miten se palvelee yrityksen liiketoimintaa.

Tietoturvan nykytilan vuoksi organisaation tulisi aloittaa selkeä ohjelma, jonka kautta yrityksessä käynnistyisi selkeä tietoturvallisuuden prosessi. Toimipisteen johdon tulisi selvittää itselleen tietoturvatyöhön kuuluvat vastuut ja määrittää niitä eri henkilöille tarvittaessa. Joskus yrityksen organisaatiorakennetta on muutettava, jotta vastuunjako pystytään toteuttamaan mahdollisimman tehokkaalla tavalla. Myöskin henkilökunnalle tulisi tehdä selväksi mitkä heidän vastuunsa ovat ja miten ne vaikuttavat heidän nykyisiin työtehtäviinsä. Olisi hyvä, että yritys olisi valmis näihin muutoksiin ja antamaan täyden tukensa henkilökunnalle uusien vastuiden noudattamisen saralla. Tavoite olisi se, että tietoturvatyö saataisiin integroitua yrityksen päivittäisiin toimiin ja organisaatio pystyisi toimimaan tietoturvan vastuiden mukaisella tavalla liiketoiminnan muuttuvissa olosuhteissa.

Tämän lisäksi kohdeorganisaatiolla tulisi olla työtehtäväkohtaiset ohjeet tietoturvaan liittyen, jotta henkilöstön toiminta palvelisi parhaalla mahdollisella tavalla liiketoiminnan jatkuvuutta, mutta olisi tietoturvan kannalta oikeita toimintatapoja noudattavaa. Suoraviivainen ja yksiselitteinen, kaikkien saatavilla oleva tietoturvaohje karsii tehokkaasti tietämättömyydestä johtuvat virheet ja

toimintatavat. Lisäksi tarkat ohjeet ovat paras tapa saada tietoturvakäytännöt sisällytettyä jokapäiväiseen toimintaan. Myös muun tietoturvallisuuteen liittyvän dokumentaation ylläpitämistä voisi harkita kohdeorganisaatiossa kehitettävän, sillä tietoturvatyön kehittäminen on oleellisesti helpompaa, jos sen vaatima informaatio on jo valmiiksi kerätty talteen työtä varten.

Henkilöstön kouluttaminen tietoturvallisuuteen liittyvillä ohjeilla on myös tärkeää, jotta he omaksuisivat myönteisin mielin toimintatavat osaksi päivittäisiä rutiinejaan ja ymmärtäisivät niiden tärkeyden ja tavoitteet. Yrityksen tulisi myös panostaa salasanaohjeistukseen, jossa määritellään yksinkertaiset ohjeet salasanojen luomiseen, vaihtoon ja säilytykseen, sekä johon sisällytetään kiellot esimerkiksi salasanojen uusiokäyttöön. Tämän ohjeistuksen tulisi olla kaikkien saatavilla ja esillä aina salasanan vaihdon yhteydessä. Asia hoituisi jos yritys kehittäisi pitkäaikaisen tietoturvallisuustyön kautta itselleen tietoturvapolitiikan ja -suunnitelmat, sekä tietoturvaohjeet. Tietoaineistoturvallisuuden korjaamiseksi yritys voisi luoda ohjeen josta ilmenee tiedon elinkaarta kuvaava prosessi kaikkine vaiheineen, jotta kaikki organisaation työntekijät sitä hyödyntäen osaisivat toimia oikein tiedon käsittelyyn ja tuhoamiseen liittyvissä asioissa.

4.3 Palomuurin nykytila

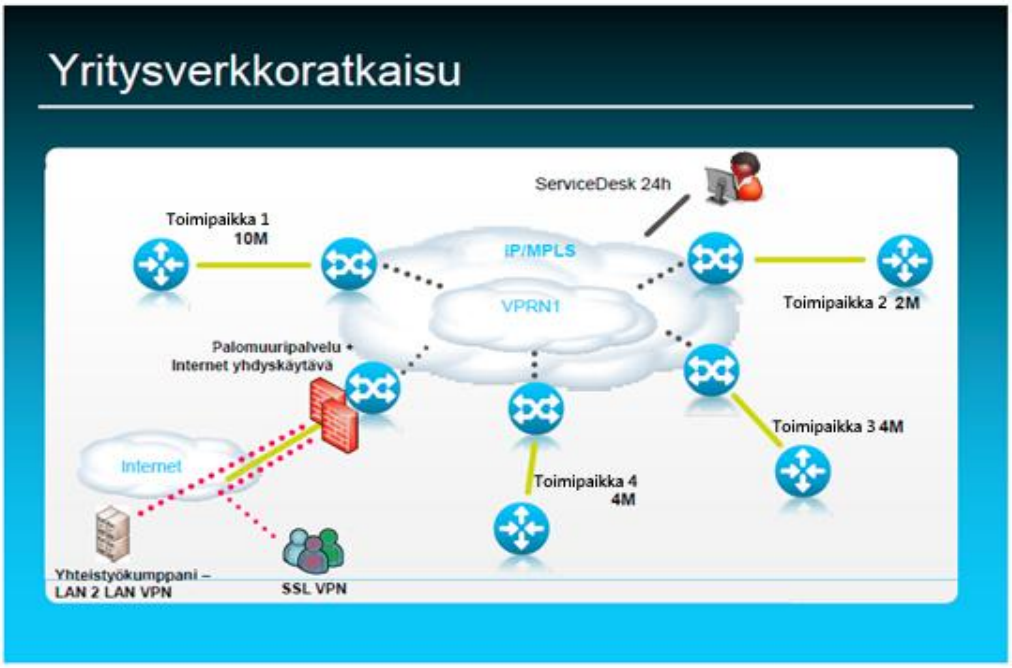
Ulkoisena palomuurina kohdeorganisaatio on turvautunut käyttämään GNAT -merkkistä laitepalomuuria. GNAT Boxia voidaan hallita joko komentoriviltä tai www-käyttöliittymän kautta. Se suodattaa saapuvan liikenteen lähde-IP-osoitteen, kohdeosoitteiden, portin, verkkoliitännän ja protokollan perusteella. “Rautapohjaisen” palomuurin etuna on se, että murtautumisen vaara on pienempi sen sisältäessä vähälukuisesti ohjelmia, joista hyökkääjä voi löytää tietoturva-aukkoja ja hyökkääjän on siten vaikeaa päästä muokkaamaan palomuurin asetuksia. Laitepalomuurihankinta on tehty vuonna 2004 ja organisaatio on harkinnut uuteenpanostamista, vaikka haastattelun mukaan vanhallakin on tultu hyvin toimeen. Uuteen haluttiin paremmat VPN-ominaisuudet, jotta etätyöskentelyä voitaisiin kehittää.

Työntekijöiden käyttämissä tietokoneissa virus- ja palomuuriohjelma vaihtelee eri ilmaisohjelmistojen välillä. Kohdeorganisaatio on yrittänyt välttää raskaampia virustorjuntaohjelmia ja siirtynyt kevyempiin ilmaiseksi ladattaviin ohjelmistoihin.

4.4 Tarjoukset ja ehdotukset

Operaattoripohjainen tarjous kohdeyritykselle :

Operaattori tarjosi kohdeyritykselle kuvion 6 mukaista yritysverkkoratkaisua ja palomuuripalvelua. Toteutus perustuu IP/MPLS tekniikkaan, jonka avulla pystytään yhdistämään useat eri toimipaikat yhdeksi sisäverkoksi, vaikka toimipisteet sijaitsisivat eri puolella Suomea. Tässä vaihtoehdossa kohdeyrityksen tiloissa ei olisi konkreettista palomuuria, vaan se sijaitsisi palveluntarjoajan tiloissa. Ongelmatilanteissa ServiceDesk palvelee vuorokauden ympäri. Kuvassa myös eri toimipisteiden yhteyksien nopeudet.



Kuvio 6. Yritysverkkoratkaisun infrastruktuuri.

Yksityisen tarjous kohdeyritykselle :

Tietoliikenneverkkojen asennus asiakkaan yhteen tai useampaan toimipaikkaan.

Yksityisen yrityksen taholta saatu tarjous tarjoaa sisäverkkoon Linux-palomuureihin perustuvaa ratkaisua. Jokaiseen toimipaikkaan asennetaan Linux-palomuuri ja palomuurien välille muodostetaan Ipsec–VPN-yhteys. Tällöin kaikkien toimipaikkojen tietokoneet ”näkevät” toisensa ja voivat käyttää toisissa toimipaikoissa olevia resursseja, kuten esimerkiksi jaettuja kansioita, tulostimia tai ohjelmia. Jokaisella toimipaikalla pitää olla nopea Internet-yhteys ja kiinteä IP-osoite.

Yhteyden nopeus pitää olla vähintään 8Mt sisään ja 1Mt ulospäin. Yritys tarjoaa lisäksi palomuurien ylläpidon kiinteällä kuukausimaksulla palveluna erillisellä palvelusopimuksella.

Tarjous sisältää Linux-käyttöjärjestelmään perustuvan palomuurilaitteiston sekä käyttöönasennuksen.

Linux-palomuuri, Ipsec

Ohjelmistossa mukana seuraavat ominaisuudet:

- Ipsec –VPN

Mahdollistaan useiden toimipaikkojen kytkemisen samaan lähiverkkoon.

- PPTP–VPN etätyömahdollisuus

Mahdollistaa työntekijöiden liittymisen työpaikan verkkoon missä tahansa Internet-yhteydessä olevasta tietokoneesta, jossa on PPTP–VPN -yhteysmahdollisuus.

- Palomuuri

Mahdollista rajoittaa Internetin käyttöä sisään ja ulospäin. Esim. estetään kaikki sisäänpäin tuleva liikenne ja sallitaan ulospäin vain tietyt Internet-osoitteet.

- Porttiohjaukset

Mahdollista luoda sääntöjä ja porttiohjauksia ulkoa sisäverkkoon.

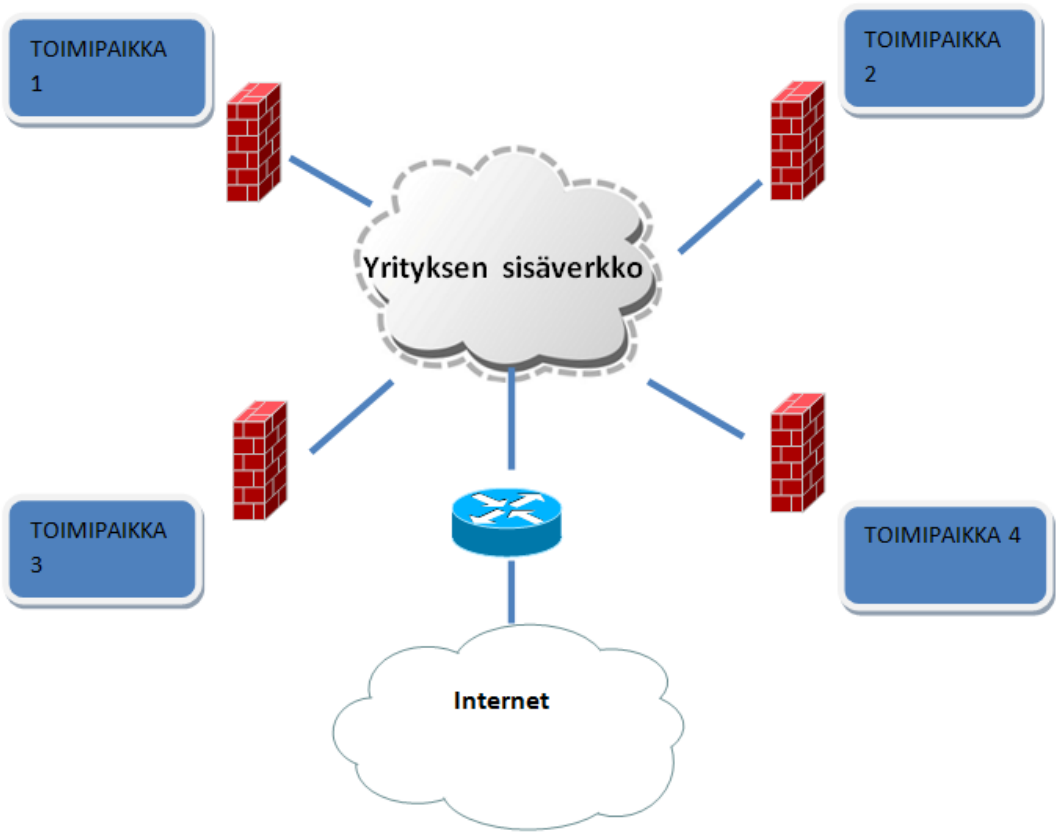
- Tunkeutumisen esto

Automaattinen murtautumisyritysten valvonta.

- Verkonhallinta

Mahdollistaa verkon jakamisen eri osiin. Esim. yritysverkko ja vierasverkko. Vaatii 802.1Q tuen.

Kuviossa 7 havainnollistetaan yksityisen yrityksen tarjousta kohdeyrityksen tietoturvaratkaisuksi. Tässä mallissa jokaisessa toimipaikassa olisi oma kiinteä palomuuri.



Kuva 7. Yksityisen verkkoratkaisu.

Oma ehdotuksemme kohdeyritykselle:

Tarjousten analysoiminen osottautui haasteelliseksi siitä syystä, että tarjoukset eivät olleet keskenään suoraan vertailtavissa. Emme saaneet kaikkia hintatietoja käsiimme, vaan jouduimme muodostamaan analyysimme osin puutteellisen informaation perusteella. Tämä siksi koska valtakunnallisen operaattorin hintatiedoissa ei ilmennyt selkeästi, kuinka paljon asennustöitä jouduttaisiin tekemään ja kuinka paljon se maksaisi. Yksityiseltä taholta saatu tarjous sisälsi laajalti informaatiota sen sisällöstä, asennuskustannuksista ja muista hinnoista.

Ehdotetuista vaihtoehdoista mielestämme paremman vastineen rahoille tarjoaa Yritys 2, jonka ratkaisu perustuu siihen, että jokaiseen toimipaikkaan tulee oma palomuuri jotka muodostavat keskenään verkon IPsec–VPN yhteyden avulla. Pienemmässä yrityksessä asioista pystyy soittamaan suoraan sille henkilölle joka asioista on suoraan vastuussa, verrattuna siihen että ottaessasi yhteyden ensin operaattorin asiakaspalveluun pääset vasta kertomaan ongelmasi, jonka jälkeen ongelmasi kirjataan ylös ja ohjataan mahdollisesti oikean henkilön hoidettavaksi kenties viikkojen jonotuksen päähän. On toki mahdollista räätälöidä sopimus jonka perusteella on mahdollisuus saada ongelmiin ratkaisu jo tunnin kuluessa, mutta tällaiset sopimukset ovat erittäin kalliita. Tietoturvallisuuden näkökulmasta parempi ratkaisu on myös se, että palomuuri sijaitsee yrityksen omissa tiloissa eikä siihen varmasti pääse koskemaan yksikään henkilö yrityksen niin halutessa. Palomuurin sijaitessa operaattorin tiloissa voimme vain luottaa siihen, että yritys hoitaa vastuunsa palomuurilaitteista asiaankuuluvalla tavalla.

5 YHTEENVETO

Yrityksen tietototurvallisuuden tason selvittäminen on perusteltua aikana, jolloin yritysten tietoturvallisuuteen pitää kiinnittää yhä enemmän huomiota. Tietoturvakartoitus tarjoaa toteuttajalleen erilaisten testauksien kautta kattavan kuvan oman tietoturvansa tilasta käytössä olevien tietotekniikkaratkaisujen osalta, raportin havaituista ongelmista ja puutteista sekä niiden parannukseen räätälöidyt ratkaisut. Suorittamamme suppeampi tietoturvatyö ei sisältänyt edellä mainittuja testauksia, vain nykyisen palomuurin, virustorjuntaohjelmiston ja laitteiston katselmoinnin, sekä parannukseen tarvittavan ratkaisun, joka oli toisen teleoperaattorin tarjoama, yrityksille suunnattu tietoturva –ja laajakaistapalvelu.

Yrityksiin kohdistuvat tietoturvariskit voivat toteutuessaan vaikuttaa liiketoimintaan ja sen tulokseen, jopa estää koko liiketoiminnan jatkuvuuden. Lisäksi se antaa huonoa mainosta yritykselle ja vaikuttaa sekä vanhoihin että uusiin asiakasuhteisiin negatiivisella tavalla. Tietoturvakartoituksen tarkoitus onkin minimoida nämä riskit. Onnistuimme valitsemamme lähestymistavan avulla tekemään kartoituksen loppuun ja kohdeyritys päätyi sitä miellyttävään ratkaisuun, jossa siihen kohdistuvat tietoturvariskit minimoitiin kustannusten kuitenkin pysyessä mahdollisimman alhaisina.

Tietoturvakartoituksen toteutukseen siirryttäessä on tärkeää, että työ on räätälöity juuri kohdeyrityksen käyttöön sopivaksi ja tarkoituksenmukaiseksi. Tämä taataan analyysien ja haastattelujen kautta, sillä niiden tuloksista ilmenee kohdeyrityksen käytössä olevat tekniikat kuten mm. käyttöjärjestelmät, tietojen näkyvyys, tunkeutumisen mahdollisuudet, palomuurien ja aktiivilaitteiden sijoitus sekä niiden määritelmät. Kohdeyrityksen tiedot tulivat meille lopulta melko hyvin selväksi kyseisten haastatteluiden kautta, joskin hieman nihkeästi ja useiden eri haastattelujen kautta. Lisäkysymysten herätessä asiat hoidettiin puhelimen sekä uusien kokouksien välityksellä. Saatujen tietojen avulla pääsimme viimein aloittamaan työn. Myös henkilökunnan asenne tietoturvaan ja tietoturvaohjeiden noudattamiseen ilmenee kartoituksessa ja tuloksista riippuen johtaa yleensä

jatkotoimenpiteisiin ja/tai seurantaan. Kohdeyrityksessä henkilökunta oli asenteeltaan samaa tasoa kuin heidän noudattamansa ”tietoturvapolitiikka”, jota ei ollut paperilla ollenkaan, vaan se oli pikemminkin heille kehittynyt tapa toimia. Eli yrityksessä ei täysin tiedosteta mikä merkitys tietoturvalla nykypäivänä on. Asia ei kuitenkaan ole noussut tai ollut noussut ongelmaksi. Henkilökunnalle loimme perusasiat sisältävän tietoturvaohjeen tueksi (Liite 1) jokapäiväiseen toimintaan. Laajin tietämys käytössä olevasta tekniikoista ja tietoturvasta oli kohdeorganisaation yhteyshenkilöllä, jolta toimeksiannon saimme ja häntä me pääasiassa haastattelimmekin.

Toteutusvaiheessa tietoturvakartoituksessa kerättyjen tietojen perusteella ryhdytään toimiin. Tietoturvaohjeet käydään läpi ja puutteiden ilmetessä ne voidaan joutua päivittämään tai jopa luomaan kokonaan alusta alkaen. Järjestelmät, sovellukset ja laitteisto päivitetään ajan tasalle, tai vaihdetaan uusiin. Henkilökunta ohjeistetaan tai koulutetaan uusien toimintamallien tasalle. Työssämme kohdeyrityksen ohjelmistolle ja laitteistolle kävikin juuri näin ja ne vaihdetaan uusiin kun sopimus teleoperaattorin kanssa on tehty. Lähtökohdat kartoituksen toteuttamisen laajuudelle riippuuvatkin paljon yrityksen koosta ja aiemmista toimintatavoista, sillä pienemmissä yrityksissä, kuten meidän tapauksessamme, tietoturvakäytännöt voivat olla niin alkutekijöissään, että moni asia täytyy luoda yritykselle alusta alkaen. Tietoturvakartoitus voi helposti johtaa hyvin suuritöiseksi projektiksi, joten sen toteuttajilla tulee olla hyvät resurssit ja valmiudet. Meillä ei laajaan projektiin niitä ollut ja siksi päädyimmekin toteuttamaan kartoituksen sopimallamme suppealla tavalla.

Jokainen yritys käyttää tietotekniikkaa, koosta riippumatta. Se on nykyään olennainen osa liiketoimintaa ja siksi tietoturvakartoitus on yhtä olennainen osa modernien yritysten tietoturvan työkaluja. Kartoitusta ei tehdä turhaan, sillä asiantuntijoiden suorittamana sen tuloksista selviävät kaikki tarpeet tietoturvalle kohtuullisin kustannuksin. Toteuttamassamme kartoituksessa toivoimmekin, että pystyimme tarjoamaan kohdeyritykselle kaivattua hyötyä kartoituksen muodossa, vaikka emme ammattilaisia olekaan. Kartoitusta ei tehdä vain yhden kerran, sillä jatkuva muutos tuo aina uusia aukkoja ja potentiaalisia

haavoittuvuuksia. Tästä syystä tietoturva tarvitsee säännöllistä seurantaa sekä toimenpiteitä.

Tekemämmme tietoturvatyö antaa yritykselle hyvän lähtökohdan jatkaa päivittäistä työtä tietoturvan parantamiseksi. Kuitenkin täyden varmuuden tietoturvastaan yritys saisi, jos yritys antaisi asiantuntevalle yritykselle toimeksiannon laajamittaisemman tietoturvakartoituksen tekemiseksi. Suorittamalla tämän kartoituksen, kohdeorganisaatio saisi hyvän kuvan mahdollisesta tarpeestaan tietoturvalle kohtuullisin kustannuksin, sillä nykyään tietotekniikka on olennainen osa kaikkea liiketoimintaa. Tekemämme tietoturvatyössä esille saatujen tietojen perusteella voimme jo sanoa, että yritys on oikealla polulla tietoturva-asioidensa hoitamisen suhteen, mutta se tarvitsee vielä tarkemmat määritelmät tietoturvapolitiikan- ja ohjeiden muodossa, sekä tietoturvan toteutumiseen yksilötasolla.

6 POHDINTA

Kun katselimme erilaisia tietoturvakartoituksia sekä ohjeistuksia, huomasimme niiden olevan pääasiassa tarkoitettu paljon suurempien organisaatioiden käyttöön. Opinnäytetyön onnistumisen kannalta ja toimeksiantajana toimivan pk-yrityksen näkökulmasta ei kannata, eikä ole kustannustehokasta muodostaa laajaa tietoturvaprojektia, jonka parissa useat henkilöt työskentelisivät pitkällä aikavälillä. Resurssien ja aikataulun takia pienemmän mittakaavan projekti on tässä tilanteessa järkevämpi vaihtoehto.

Työn aihe muuttui sen kehittyessä. Aluksi oli tarkoitus tehdä itse tarvittavat muutokset yrityksen tietoturvaan ja palomuuriin, kun tarvittavat ongelmakohdat kartoituksen jälkeen löytyvät. Pian kuitenkin tajusimme työn olevan liian suuri opinnäytetyöksi ja työ itsessään olisi erittäin vaativa. Tästä syystä aihe muuttui niin, että annamme kohdeorganisaatiolle vain ehdotuksen siitä, miten heidän tulisi muuttaa tietoturvaan liittyviä käytäntöjään, jotta yrityksessä tunnistetaan ne tiedot, jotka halutaan salata asiaan kuuluvalla tavalla.

Tiedonkeruumenetelmänä on käytetty suullisia haastatteluja (Liite 2) koska meidän käyttöömme ei annettu yksityiskohtaista tietoa yrityksen tietoverkon infrastruktuurista tai muista laitteista. Emme saaneet tarkastella laitteita, emmekä myös saaneet yksityiskohtaista dokumentaatiota käsiimme. Saadut tiedot olivat kuitenkin siinä mielessä riittäviä, jotta teorian ja kerättyjen tietojen perusteella voidaan tehdä olettamus siitä, missä kohdeorganisaation mahdolliset heikkoudet sijaitsevat ja mitä he tarvitsevat niiden paikkaamiseen.

Oma ymmärryksemme tietoturvasta kasvoi nähtyämme miten yritys käytännön tasolla toimii ja mitkä asiat näyttäytyvät yrityksessä tärkeimpinä. Lisäksi perehdyimme asiaan tarkasti myös kirjallisuuden avulla. Opinnäytetyö oli hyvä mahdollisuus peilata omia kokemuksiamme koulun tarjoamien kurssien pohjalta, sekä laajentaa tietämystä ja nähdä miten tietoturvatyötä tehdään yrityksessä.

LÄHTEET

Cygate. Tietoturvaratkaisut. Hakupäivä: 15.9.2012, http://www.cygategroup.com/templates/Page.aspx?id=1025

Hakala, M. & Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docento Finland Oy

Internet verkon käyttötavat ja niiden tietoturvallinen toteutus. Hakupäivä: 15.9.2012, https://www.vahtiohje.fi/web/guest/internet-verkon-kayttotavat-ja-niiden-tietoturvallinen-toteutus

Järvinen, P. 2002. tarkista Tietoturva & yksityisyys. Jyväskylä: Docendo Finland Oy

Järvinen, P. 2005. Yrityksen tietoturvapolitiikka. Hakupäivä: 1.4.2012, http://www.tietokone.fi/lehti/tietokone_1_2005/yrityksen_tietoturvapolitiikka_2610

Kyrölä, T. 2001. Esimies ja tietoriskien hallinta. Helsinki: WSOY

Laaksonen, M. & Nevasalo, T. & Tomula, K. 2006 tarkista. Yrityksen tietoturvakäsikirja. Helsinki: Edita Puplishing Oy

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Helsinki: Talentum.

Puhakainen, P. 2006. A desing theory for information security awareness.

Ruohonen, M. 2002. Tietoturva. Jyväskylä: Docento Finland Oy

Schneier, B. 2004. Secrets and lies. Indianapolis, IN, Yhdysvallat: Wiley Publishing

Simsala Team Oy. Tietoturvakartoitus. Hakupäivä: 31.1.2012, http://www.simsala.net/tietoturva_kartoitus_1.htm

Stallings, W. 2006. Cryptography and network security. Upper Saddle River, NJ, Yhdysvallat: Pearson Education.

Suominen, A. Riskienhallinta. 2003. Helsinki : WSOY

Tietoturva 2012. Tilanteen kartoitus; tiedon luokittelu. Hakupäivä: 30.4.2012, http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/tiedon_luokittelu.html

Työturvallisuuskeskus 2012. Vaarojen tunnistaminen ja riskien arviointi. Hakupäivä 17.3.2012, http://www.ttk.fi/riskienarviointi

Valtiovarainministeriö 2003. Valtiohallinnon tietoturvakäsitteistö. Hakupäivä 4.6.2012, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf

Valtiovarainministeriö 2006. Henkilöstön tietoturvaohje. Hakupäivä 13.5.2012. http://www.oulu.fi/tietohallinto/tietoturva/sisalto/kayton_ohjeet/VAHTI/Vahti_10_06.pdf

Valtiovarainministeriö 2009. Henkilöstöturvallisuus. Hakupäivä 1.3.2012 https://www.vahtiohje.fi/web/guest/henkilostoturvallisuus;jsessionid=B92B777615EA80AF5EE8F9A6D5465162A8EB907031B885D6AD25CA53A0C60D046AB39BC997038347B16335

Viestintävirasto 2007. Tiedon turvaamisella menestykseen. Hakupäivä: 30.4.2012, http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tiedon_turvaamisella_menestykseen_luentosarja_2007.pdf

Viestintävirasto 2007. Tilanteen kartoitus; Esimerkki käsittelyohjeista. Hakupäivä 1.3.2012.
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/kasittelyohjeet.html

Virtanen, T, 2004. Talon turvaopas. Helsinki: Savion kirjapaino

Von Solms, B. 2000. Information Security – The Third Wave. Amsterdam, Hollanti.

LIITTEET

LIITE 1.

TIETOTURVAOHJE

Seuraavassa on kohdeorganisaatiolle laadittu yleinen tietoturvaohje, koskien henkilökunnan päivittäistä tietojenkäsittelyä ja siinä huomioonotettavia seikkoja, jotta vältyttäisiin perustavanlaatuisilta ongelmilta.

Keskeiset ohjeet :

1. Estä asiaton pääsy tietojärjestelmiin lukitsemalla koneesi aina, kun poistut työhuoneestasi.
2. Älä jätä vierasta yksin tai valvomatta työhuoneeseesi tai muihin organisaation tiloihin. Älä anna ulkopuolisen käyttää tietokonettasi.
3. Noudata ns. puhtaan pöydän periaatetta. Älä säilytä työpöydälläsi luottamuksellista aineistoa.
4. Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen jokapäiväisten nimien käyttöä salasanana. Vaihda salasanaa muutaman kerran vuodessa ja heti, jos epäilet sen paljastuneen. Älä säilytä salasanaa muistilapulla näkyvällä paikalla.
5. Internet ja sähköposti on työpaikalla tarkoitettu työkäyttöön.
6. Internetin kautta ei ole luvallista välittää salassa pidettävää tietoa ilman ajanmukaista salausta.
7. Liitetiedostot voivat sisältää haittaohjelmia (Viruksia, matoja tai troijalaisia). Älä avaa sähköposteja joiden lähettäjää et tunne ja erityisesti sähköpostien liitetiedostoja.
8. USB-muistitikut, ja CD- ja DVD -levyt voivat sisältää suuria määriä luottamuksellista tietoa. Säilytä siis USB-muistitikuilla mukana vain sillä hetkellä tarvitsemasi tiedot. Älä käytä muistitikkua ns. yleisvarastona, se ei ole tiedon ensisijainen tallennuspaikka.

9. Älä asenna ohjelmistoja tai tee niiden asetusmuutoksia, ellei tämä kuulu varsinaisiin työtehtäviisi.
10. Työpäivän päätteeksi kirjaudu tietojärjestelmästä ulos ja sammuta työasemasi.
11. Pyydä tarvittaessa neuvoa organisaatiosi asiantuntijoilta.

LIITE 2.

HAASTATTELURUNKO

1. Kerro yrityksestä ja sen toiminnasta yleisesti.

2. Miten toivot/arvelet tietoturvakartoituksen hyödyttävän yrityksenne toimintaa?

3. Onko yrityksen työasemat liitetty toimialueeseen?

4. Miten yrityksen tiedostojen jakelu on hoidettu?

5. Minkälaiset etätyöskentelymahdollisuudet työntekijöillä on?

6. Miten yrityksen virustorjunta on järjestetty työasemissa?

7. Kuinka yrityksen työntekijöitä on ohjeistettu tietoturva-asioissa?

8. Millaiset ATK-taidot henkilökunnalla on yleisesti?

9. Kuka vastaa esimerkiksi palomuurien ylläpidosta?

10. Millaiset palvelimet yrityksellä on käytössä?

11. Onko kaikissa toimipisteissä oma palvelin?

12. Kuka on nykyinen palveluntarjoaja?

13. Onko kaikilla toimipisteillä käytössä sama palomuuri?

14. Kuinka tietojärjestelmä- ja tietoturva-asiat on dokumentoitu (laitteiden elinkaaret jne.)?

15. Miten varmuuskopiointi on hoidettu?

16. Miten sijaisuusasiat ovat järjestetty?

17. Miten koneiden käyttöoikeudet on hoidettu?

18. Mitä sähköpostiohjelmaa henkilökunta käyttää?

19. Mitä toiveita uuden palveluntarjoajan suhteen yrityksellä on esimerkiksi palvelujen osalta?

20. Miten haluat hoitaa kartoituksesta saatujen tuloksien julkistamisasiat?